Common Vulnerability Scoring System version 4.0

Examples

Document Version: 1.0

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of four metric groups: Base, Threat, Environmental, and Supplemental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Threat group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. Base metric values are combined with default values that assume the highest severity for Threat and Environmental metrics to produce a score ranging from 0 to 10. To further refine a resulting severity score, Threat and Environmental metrics can then be amended based on applicable threat intelligence and environmental considerations. Supplemental metrics do not modify the final score, and are used as additional insight into the characteristics of a vulnerability. A CVSS vector string consists of a compressed textual representation of the values used to derive the score. This document provides the official specification for CVSS version 4.0.

Contents

Resources & Links

Below are useful references to additional CVSS v4.0 documents.

Resource	Location
Specification Document	Includes metric descriptions, formulas, and vector strings. Available at https://www.first.org/cvss/v4.0/specification-document
User Guide	Includes further discussion of CVSS v4.0, a scoring rubric, and a glossary. Available at https://www.first.org/cvss/v4.0/user-guide
Examples Document	Includes examples of CVSS v4.0 scoring in practice. Available at https://www.first.org/cvss/v4.0/examples
CVSS v4.0 Calculator	Reference implementation of the CVSS v4.0 equations, available at https://www.first.org/cvss/calculator/4.0
JSON & XML Data Representations	Schema definition available at https://www.first.org/cvss/data-representations
CVSS v4.0 Main Page	Main page for all other CVSS resources: https://www.first.org/cvss/v4-0/

Introduction

This document demonstrates how to apply the CVSS version 4.0 standard to assess specific vulnerabilities. Every vulnerability example includes a summary and a breakdown of the assessment. CVSS version 3.0 scores are provided to show differences between the two standards.

Details of the vulnerabilities and attacks were sourced primarily from the National Vulnerability Database (NVD) at https://nvd.nist.gov/vuln/search. Information from additional sources was also used when more details were required.

Common Vulnerability Scoring System version 4.0 Examples

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of four metric groups: Base, Threat, Environmental, and Supplemental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Threat group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. Base metric values are combined with default values that assume the highest severity for Threat and Environmental metrics to produce a score ranging from 0 to 10. To further refine a resulting severity score, Threat and Environmental metrics can then be amended based on applicable threat intelligence and environmental considerations. Supplemental metrics do not modify the final score, and are used as additional insight into the characteristics of a vulnerability. A CVSS vector string consists of a compressed textual representation of the values used to derive the score. This document provides the official specification for CVSS version 4.0.

The most current CVSS resources can be found at https://www.first.org/cvss/

New metric coverage

This section includes scoring examples that illustrate aspects of changed or modified metrics.

New Metric – Attack Requirements

CVE-2022-41741

A vulnerability in the module ngx_http_mp4_module might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module.

v3.1	**v4.0 Base**
7.0	7.3
CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVSS v4 Score: Base 7.3

Metric	Value	Comments

Attack Vector	Local	An attacker must be able to access the vulnerable system with a local, interactive session.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	Present	NGINX must be built with the module, *and* configuration must be present. Neither of those are default scenarios for an NGINX OSS web server. The attacker must place a file within the web root and cause NGINX to serve that file.
Privileges Required	Low	An attacker must be able to place a file within the web root to be processed by NGINX.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	The attacker could execute arbitrary code on the vulnerable system with elevated privileges.
Vulnerable System Integrity	High	The attacker could execute arbitrary code on the vulnerable system with elevated privileges.
Vulnerable System Availability	High	The attacker could execute arbitrary code on the vulnerable system with elevated privileges.
Subsequent System Confidentiality	None	There is no impact to the subsequent system confidentiality.
Subsequent System Integrity	None	There is no impact to the subsequent system integrity.
Subsequent System Availability	None	There is no impact to the subsequent system availability.

CVE-2020-3549

A vulnerability in the sftunnel functionality of Cisco Firepower Management Center (FMC) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to obtain the device registration hash.

The vulnerability is due to insufficient sftunnel negotiation protection during initial device registration. An attacker in a man-in-the-middle position could exploit this vulnerability by intercepting a specific flow of the sftunnel communication between an FMC device and an FTD device. A successful exploit could allow the attacker to decrypt and modify the sftunnel communication between FMC and FTD devices, allowing the attacker to modify configuration data sent from an FMC device to an FTD device or alert data sent from an FTD device to an FMC device.

	v3.1	**v4.0**
Base	8.1 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	7.7 CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
Base + Threat		5.2 CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U

CVSS v4 Score: Base + Threat 5.2

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	Present	An attacker must be on-path to be able to intercept communications between affected systems.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	Passive	A user must be logged in and using the application for traffic to be generated that an attacker could capture.
Vulnerable System Confidentiality	High	An attacker could gain access to the system with a highly privileged user account.

Vulnerable System Integrity	High	An attacker could gain access to the system with a highly privileged user account.
Vulnerable System Availability	High	An attacker could gain access to the system with a highly privileged user account.
Subsequent System Confidentiality	None	There is no impact to the vulnerable system confidentiality.
Subsequent System Integrity	None	There is no impact to the vulnerable system integrity.
Subsequent System Availability	None	There is no impact to the vulnerable system availability.
Exploit Maturity	Unreported	There is no known proof-of-concept code or malicious exploitation of this vulnerability.

CVE-2023-3089

Description: A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated.

	v3.1	**v4.0**
Base	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	8.3 CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N
Base + Environmental		8.1 CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N/CR:H/IR:L/AR:L/MAV:N/MAC:H/MVC:H/MVI:L/MVA:L

CVSS v4 Score: Base + Environmental 8.1

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	There is no inherent vulnerability, but a lower level of cryptography than expected was being used, resulting in a lower-than-configured certificate security.
Attack Requirements	Present	Attack requirements are present. Only applications built with a specific configuration are vulnerable.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	This CVE particularly affects high-security systems (FIPS users) and lowers the requirements to access confidential information.
Vulnerable System Integrity	Low	Integrity will be at a lower cryptographic level than desired, but is still always encrypted.
Vulnerable System Availability	Low	Integrity will be at a lower cryptographic level than desired, but is still always encrypted.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.
Modified Attack Vector	Network	This still requires spoofing a cryptographically secure certificate, just not always an FIPS-approved algorithm.
Modified Attack Complexity	High	This still requires spoofing a cryptographically secure certificate, just not always an FIPS-approved algorithm.
Modified Vulnerable System Confidentiality	High	This still requires spoofing a cryptographically secure certificate, just not always an FIPS-approved algorithm.

Modified Vulnerable System Integrity	Low	Integrity will be at a lower cryptographic level than desired, but is still always encrypted.
Modified Vulnerable System Availability	Low	Integrity will be at a lower cryptographic level than desired, but is still always encrypted.
Confidentiality Requirements	High	System certificates are still encrypted correctly, but at a weaker level than expected, resulting in a hard-to-abuse system, but easier than intended/designed for the system.
Integrity Requirements	Low	There is a low chance of integrity being modified, but higher than expected behavior.
Availability Requirements	Low	There is a low chance of availability being affected, but higher than expected behavior.

Revised Metric – User Interaction

Analysts assessing User Interaction should consider the necessary actions taken by a user. As per the specification document, operations normally taken by a user would be User Interaction:Passive. Actions that are out of the ordinary, against recommended guidance, or subverting security controls, would be User Interaction:Active.

CVE-2021-44714

Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a Violation of Secure Design Principles that could lead to a Security feature bypass. Acrobat Reader DC displays a warning message when a user clicks on a PDF file, which could be used by an attacker to mislead the user. In affected versions, this warning message does not include custom protocols when used by the sender. User interaction is required to abuse this vulnerability as they would need to click 'allow' on the warning message of a malicious file.

v3.1	**v4.0 Base**
3.3	4.6

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

CVSS v4 Score: Base 4.6

Metric	Value	Comments
Attack Vector	Local	The document must be present on the local disk.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	Active	User interaction is required to abuse this vulnerability because they would need to click **allow** on the warning message of a malicious file.
Vulnerable System Confidentiality	Low	Warning dialog messages do not contain all information about the document. Important omitted information about the document may allow the attacker to conduct further spoofing attacks.
Vulnerable System Integrity	None	There is no impact on vulnerable systems.
Vulnerable System Availability	None	There is no impact on vulnerable systems.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.

CVE-2022-21830

Description A blind self XSS vulnerability exists in RocketChat LiveChat <v1.9 that could allow an attacker to trick a victim pasting malicious code in their chat instance.

V3.1	**v4.0 Base**
6.1	5.1
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

CVSS v4 Score: Base 5.1

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	Active	The attacker must convince the user to input malicious script into the application.
Vulnerable System Confidentiality	None	No impact to the vulnerable application.
Vulnerable System Integrity	None	No impact to the vulnerable application.
Vulnerable System Availability	None	No impact to the vulnerable application.
Subsequent System Confidentiality	Low	An attacker could read data from the user's browser.
Subsequent System Integrity	Low	An attacker could modify data in the user's browser.

Subsequent System Availability	None	No direct availability impact to the user's browser.

New Metric – Subsequent Confidentiality, Availability, Integrity

Some examples of subsequent systems include:

- Guest host in a VMM hypervisor
- Device attached to a network gateway
- A managed Device
    - Including OT / ICS / SCADA equipment

CVE-2022-22186

Due to an Improper Initialization vulnerability in Junos OS on EX4650 devices, packets received on the em0 but not destined to the device, may be improperly forwarded to an egress interface, instead of being discarded. Such traffic being sent by a client may appear genuine, but is non-standard in nature and should be considered as potentially malicious.

v3.1	**v4.0 Base**
7.2	6.9
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

CVSS v4 Score: Base 6.9

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	An attacker must be able to access the vulnerable system with a local, interactive session.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully

		exploit the vulnerability.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	None	There is no impact to the vulnerable system confidentiality.
Vulnerable System Integrity	None	There is no impact to the vulnerable system integrity.
Vulnerable System Availability	None	There is no impact to the vulnerable system availability.
Subsequent System Confidentiality	Low	Network traffic or information from restricted hosts may be detected.
Subsequent System Integrity	Low	Network traffic may be sent to an undesired interface.
Subsequent System Availability	None	There is no impact to subsequent systems.

CVE-2023-21989

Description

Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attackers with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data.

v3.1	**v4.0 Base**
6.0	5.9
CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA:N

CVSS v4 Score: Base 5.9

Metric	Value	Comments
Attack Vector	Local	An attacker must be able to access the vulnerable system with a local, interactive session.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	High	An attacker must have administrative control over a virtual machine within the virtual machine host.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	None	There is no impact to the vulnerable system confidentiality.
Vulnerable System Integrity	None	There is no impact to the vulnerable system integrity.
Vulnerable System Availability	None	There is no impact to the vulnerable system availability.
Subsequent System Confidentiality	High	An attacker could exploit this vulnerability to access confidential information stored within the VM host hypervisor system.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.

CVE-2020-3947

VMware Workstation (15.x before 15.5.2) and Fusion (11.x before 11.5.2) contain a use-after vulnerability in vmnetdhcp. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition of the vmnetdhcp service running on the host machine.

v3.1	v4.0 Base
9.3	9.4
CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

CVSS v4 Score: Base 9.4

Metric	Value	Comments
Attack Vector	Local	An attacker must be able to access the vulnerable system with a local, interactive session.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	High	An attacker must have administrative control over a virtual machine within the virtual machine host.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	An attacker could execute arbitrary code on the vulnerable system.
Vulnerable System Integrity	High	An attacker could execute arbitrary code on the vulnerable system.
Vulnerable System Availability	High	An attacker could execute arbitrary code on the vulnerable system.
Subsequent System Confidentiality	High	An attacker could take actions on other systems hosted within the virtual hypervisor.
Subsequent System Integrity	High	An attacker could take actions on other systems hosted within the virtual hypervisor.
Subsequent System Availability	High	An attacker could take actions on other systems hosted within the virtual hypervisor.
Exploit Maturity	Proof-of-Concept (P)	A proof of concept is available

New Metric – Safety

Safety is a Supplemental metric which may be optionally assessed by a scoring provider with values of Not Defined (X), Present (P), or Negligible (N). In the case of a system that intends to have health-related functions, it might also have a Safety-related consequence if a vulnerability is exploited. Let's look at an example.

CVE-2023-30560

There are two known configurations of a product known as the Becton Dickinson PCU which can be modified without authentication using physical connection to the PCU. A PCU is commonly used for infusion delivery in a healthcare provider environment. With that context in mind, it could be inferred that an exploit of this vulnerability might have Safety impact. The below is only an example of how this, or a similar vulnerability, *could* be scored.

v3.1	**v4.0 Base**
6.8	8.3
CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:H/SA:N/S:P/V:D

CVSS v4 Score: Base 8.3

Metric	Value	Comments
Attack Vector	Physical	An attacker must be able to physically access the system.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	An attacker is unauthorized prior to the attack.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	An attacker could execute arbitrary code on the vulnerable system.

Vulnerable System Integrity	High	An attacker could execute arbitrary code on the vulnerable system.
Vulnerable System Availability	High	An attacker could execute arbitrary code on the vulnerable system.
Subsequent System Confidentiality	None	If the scoring provider assumes that a patient is the subsequent system, a successful exploit would not result in loss of confidentiality.
Subsequent System Integrity	High	If the scoring provider assumes that a patient is the subsequent system, a successful exploit could result in loss of health integrity for that patient.
Subsequent System Availability	None	If the scoring provider assumes that a patient is the subsequent system, the attribute of availability might be metaphorically ambiguous.

CVSS v4 Supplemental Metrics

Metric	Value	Comments
Safety	Present	Consequences of exploiting this vulnerability could have a Safety impact that is equal to or worse than “marginal”, as described in IEC 61508.
Value Density	Diffuse	The system with the vulnerable component is fairly limited in resources.

Classic Examples

These were in the previous version and we are carrying them forward to show the change between version 3 and 4.

OpenSSL Heartbleed Vulnerability (**CVE-2014-0160**)

Vulnerability

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Attack

A successful attack requires only sending a specially crafted message to a web server running OpenSSL. The attacker constructs a malformed “heartbeat request” with a large field length and small payload size. The vulnerable server does not validate the length of the payload against the provided field length and will return up to 64 kB of server memory to the attacker. It is likely that this memory was previously utilized by OpenSSL. Data returned may contain sensitive information such as encryption keys or user names and passwords that could be used by the attacker to launch further attacks

v3.1	**v4.0 Base + Threat**
7.5	8.7
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:A

CVSS v4 Score: Base + Threat 8.7

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	None	No user interaction is required for an attacker to

		successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	Access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact to the affected scope (e.g. the attacker can read the administrator's password, or private keys in memory are disclosed to the attacker).
Vulnerable System Integrity	None	There is no impact to the vulnerable system integrity.
Vulnerable System Availability	None	There is no impact to the vulnerable system availability.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.
Exploit Maturity	Attacked	There are known exploits in the wild.

Apache log4j JNDI Command Execution “log4shell” Vulnerability (**CVE-2021-44228**)

A vulnerability in the Apache log4j library could allow an unauthenticated, remote attacker to execute arbitrary commands with the privileges of the service using the vulnerable library.

v3.1 Base	**v4.0 Base + Threat**
10.0	10.0
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:A

CVSS v3.1 Base Score: 10.0

Metric	Value	Comments
Attack Vector	Network	The vulnerability is in a network service that uses log4j.
Attack Complexity	Low	No conditions outside of the user's control.
Privileges Required	None	An attacker requires no privileges to mount an attack.
User Interaction	None	The attacker requires no user interaction to successfully exploit the vulnerability
Scope	Changed	The vulnerable component could allow an attacker to affect downstream components and systems.
Confidentiality	High	An attacker can execute arbitrary commands with elevated privileges.
Integrity	High	An attacker can execute arbitrary commands with elevated privileges.
Availability	High	An attacker can execute arbitrary commands with elevated privileges.

CVSS v4 Score: Base + Threat 10.0

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	Although the attacker must prepare the environment to achieve the worst possible outcome of an attack, (for example, code execution) through control of a reachable LDAP server, the system should be assumed vulnerable.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	None	The attack does not require any user interaction.
Vulnerable System Confidentiality	High	The attacker can run arbitrary commands with elevated privileges and access sensitive system information.

Vulnerable System Integrity	High	The attacker can run arbitrary commands with elevated privileges and modify the system configuration.
Vulnerable System Availability	High	The attacker can run arbitrary commands with elevated privileges and gain access sufficient to reset or turn off the device.
Subsequent System Confidentiality	High	The attacker could exploit the vulnerability to view sensitive information from downstream systems.
Subsequent System Integrity	High	The attacker could exploit the vulnerability to modify data from downstream systems.
Subsequent System Availability	High	The attacker could exploit the vulnerability to impact the availability of downstream systems.
Exploit Maturity	Attacked	There are known exploits in the wild.

GNU Bourne-Again Shell (Bash) 'Shellshock' Vulnerability (**CVE-2014-6271**)

Vulnerability

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "Shellshock."

Attack

A successful attack can be launched by an attacker directly against the vulnerable GNU Bash shell, or in certain cases, by an unauthenticated, remote attacker through services either written in GNU Bash or services spawning GNU Bash shells. In the case of an attack against the Apache HTTP Server running dynamic content CGI modules, an attacker can submit a request while providing specially crafted commands as environment variables. These commands will be interpreted by the handler program, the GNU Bash shell, with the privilege of the running HTTPD process. As such, environment variables passed by the attacker could allow installation of software, account enumeration, denial of service, etc. Attacks against other services that have a relationship with the GNU Bash shell are similarly possible.

v3.1 Base	v4.0 Base + Threat
9.8	9.3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A

CVSS v3.1 Base Score: 9.8

Metric	Value	Comments
Attack Vector	Network	The reasonable worst-case scenario is a network attack through a web server.
Attack Complexity	Low	An attacker needs only to gain access to a listening service that uses the GNU Bash shell as an interpreter or interact with a GNU Bash shell directly.
Privileges Required	None	The reasonable worst-case scenario is an attack through a web server, which does not require any privileges, for example, a simple CGI script.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Scope	Unchanged	The vulnerable component is the GNU Bash shell, which is used as an interpreter for various services or can be accessed directly. It runs within the security authority of the operating system. The impacted component is also the operating system, so there is no scope change.
Confidentiality	High	An attacker can take complete control of the affected system.
Integrity	High	An attacker can take complete control of the affected system.
Availability	High	An attacker can take complete control of the affected system.

CVSS v4 Score: Base + Threat 9.3

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	The attacker can run arbitrary commands with elevated privileges and access sensitive system information.
Vulnerable System Integrity	High	The attacker can run arbitrary commands with elevated privileges and modify the system configuration.
Vulnerable System Availability	High	The attacker can run arbitrary commands with elevated privileges and gain access sufficient to reset or turn off the device.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.
Exploit Maturity	Attacked	There are known exploits in the wild.

Juniper Proxy ARP Denial of Service Vulnerability (CVE-2013-6014)

Vulnerability

If Proxy ARP is enabled on an unnumbered interface, an attacker can poison the ARP cache and create a bogus forwarding table entry for an IP address, effectively creating a denial of

service for that subscriber or interface. When Proxy ARP is enabled on an unnumbered interface, the router will answer any ARP message from any IP address which could lead to exploitable information disclosure. This issue can affect any product or platform running Junos OS 10.4, 11.4, 11.4X27, 12.1, 12.1X44, 12.1X45, 12.2, 12.3, or 13.1, supporting unnumbered interfaces.

Attack

Exploitation of this vulnerability requires network adjacency with the target system and the ability to generate arbitrary ARP replies sent to the connected interface. A rogue subscriber can poison the ARP cache and/or create a rogue forwarding table entry for an IP of choice, effectively obscuring that IP address or redirecting IP traffic to the attacker.

The resultant impact can be observed as unauthorized modification of a database on the vulnerable component, or as an impact on confidentiality or availability on attached devices (impacted component). Since the CVSSv3 score for a high confidentiality (or availability) impact on a changed scope is higher than a partial impact on the vulnerable component, CVSSv3 guidance recommends to score for the higher overall impact.

v3.1	**v4.0 Base**
9.3	6.4
CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:H	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:H/SI:N/SA:H

CVSS v4 Score: Base 6.4

Metric	Value	Comments
Attack Vector	Adjacent	The attacker must be within the local proximity of the device.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.

Vulnerable System Confidentiality	None	There is no impact to the vulnerable system confidentiality.
Vulnerable System Integrity	None	There is no impact to the vulnerable system integrity.
Vulnerable System Availability	None	There is no impact to the vulnerable system availability.
Subsequent System Confidentiality	High	The attacker can hijack and redirect the IP traffic to themselves.
Subsequent System Integrity	None	There is no impact to the subsequent system integrity.
Subsequent System Availability	High	Adding the rogue forwarding table can redirect the end user to rogue IP addresses.

Lenovo ThnkPwn Exploit (**CVE-2016-5729**)

Vulnerability
The SmmRuntime BIOS EFI Driver allows local administrators to execute arbitrary code with System Management Mode (SMM) privileges via unspecified vectors.

Attack
Attacker creates a buffer in memory containing exploit code to be executed in SMM context. Attacker then creates a structure with a pointer to the exploit code's entry point and triggers an SMI passing a reference to that structure. The SMM driver then calls the exploit code via the supplied function pointer.

v3.1	**v4.0 Base + Threat**
8.2	9.3
CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/R:I

CVSS v4 Score: Base + Threat 9.3

Metric	Value	Comments
Attack Vector	Local	An attacker must be able to execute code on the system.
Attack Complexity	Low	This attack leverages a failure to verify input parameters in the **SmmRuntime** driver and can be reproduced consistently with simple code.
Attack Requirements	None	No attack requirements are present.
Privileges Required	High	The attacker must be able to run kernel level (ring 0) code on the affected system.
User Interaction	None	The vulnerability is built into the BIOS and is always available. There is no user configuration involved.
Vulnerable System Confidentiality	High	SMM has complete control over the system, including all information on the system.
Vulnerable System Integrity	High	SMM access allows an attacker to modify any part of the system.
Vulnerable System Availability	High	The attacker could keep the system in SMM, denying access to the system and never returning to a normal operation mode.
Subsequent System Confidentiality	High	All software on the vulnerable system can be seen by the attacker.
Subsequent System Integrity	High	All software on the vulnerable system can be modified by the attacker.
Subsequent System Availability	High	The attacker could keep the system in SMM, denying access to software on the system.
Recovery	Irrecoverable	The attacker could keep the system in SMM, and could prevent recovery of the system by automatically running their code and locking down the system to prevent a user from accessing it.

Failure to Lock Flash on Resume from sleep (**CVE-2015-2890**)

Vulnerability
Some UEFI BIOS implementations failed to set Flash write protections such as the BIOS_CNTL locking on resume from the S3 suspend to RAM sleep state.

Attack
Attacker causes or waits until the system resumes from suspend, and then writes over the current BIOS image in Flash with a new BIOS image modified by the attacker.

v3.1	**v4.0 Base + Threat**
6.0	8.7
CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H	CVSS:4.0/AV:L/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/R:I

CVSS v4 Score: Base + Threat 8.7

Metric	Value	Comments
Attack Vector	Local	An attacker must be able to execute code on the system.
Attack Complexity	Low	An attacker has unfettered access to the Flash part on which the BIOS is stored.
Attack Requirements	Present	The vulnerability is introduced by firmware failing to enable correct flash memory protections upon the resume from S3 system sleep state.
Privileges Required	High	An attacker must be able to run kernel level (ring 0) code on the target system, in order to access the Flash part.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	An attacker that can modify the BIOS image can install components to completely monitor and control the vulnerable system.

Vulnerable System Integrity	High	An attacker that can modify the BIOS image can modify anything on the vulnerable system.
Vulnerable System Availability	High	An attacker could cause a denial of service by corrupting the BIOS image or could encrypt the vulnerable system.
Subsequent System Confidentiality	High	Any software on the system could be monitored by an agent installed in the BIOS on the vulnerable system.
Subsequent System Integrity	High	Any files on the system could be modified by an agent installed in the BIOS.
Subsequent System Availability	High	An attacker could encrypt files on the system, preventing access.
Recovery	Irrecoverable	An attacker could cause a denial of service through encryption or corruption, neither of which could be fixed by a user.

Intel DCI Issue (**CVE-2018-3652**)

Vulnerability
Existing UEFI setting restrictions for DCI (Direct Connect Interface) in 5th and 6th generation Intel Xeon Processor E3 Family, Intel Xeon Scalable processors, and Intel Xeon Processor D Family allows a limited physical presence attacker to potentially access platform secrets via debug interfaces.

Attack
An attacker with physical access can attach a debug device to the DCI interface and directly interrogate and control the processor state starting from very early in the boot process.

v3.1	**v4.0 Base**
7.6	8.6
CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

CVSS v4 Score: Base 8.6

Metric	Value	Comments
Attack Vector	Physical	An attacker must have physical access to the DCI port in order to attach the debugging device.
Attack Complexity	Low	The debugging device is off-the-shelf hardware that can be purchased from Intel.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	Only physical presence is required; no system privileges are required.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	An attacker can view all memory and CPU instructions.
Vulnerable System Integrity	High	An attacker can modify all contents of memory and control the CPU directly.
Vulnerable System Availability	High	An attacker can cause a denial of service by stopping the CPU from executing the desired functionality.
Subsequent System Confidentiality	High	An attacker can view the contents of memory for programs on the vulnerable system.
Subsequent System Integrity	High	An attacker can modify the contents of memory for running applications and files on the vulnerable system.
Subsequent System Availability	High	An attacker can modify and corrupt applications on the vulnerable system.

Common Vulnerabilities Classes

This section contains examples of commonly-seen vulnerabilities from across the industry. The examples here are meant to be illustrative of common issues, but should not be considered authoritative. Unique vulnerabilities may have different impacts.

SQL Injection – **CVE-2023-30545**

Description

PrestaShop is an Open Source e-commerce web application. Prior to versions 8.0.4 and 1.7.8.9, it is possible for a user with access to the SQL Manager (Advanced Options -> Database) to arbitrarily read any file on the operating system when using SQL function `LOAD_FILE` in a `SELECT` request. This gives the user access to critical information. A patch is available in PrestaShop 8.0.4 and PS 1.7.8.9

v3.1	**v4.0 Base**
6.5	7.1
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CVSS v4 Score: Base 7.1

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	Low	Attacker has to have database access (non-root user access).
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	An attacker can read any file on the operating system
Vulnerable System Integrity	None	There is no impact to the vulnerable system integrity.
Vulnerable System Availability	None	There is no impact to the vulnerable system availability.
Subsequent System	None	There is no impact to subsequent systems Confidentiality.

Confidentiality		
Subsequent System Integrity	None	There is no impact to subsequent systems Integrity.
Subsequent System Availability	None	There is no impact to subsequent systems Availability.

On-path Attacker – **CVE-2021-23846**

Description

Firmware for Bosch devices transmits in clear text over HTTP, allowing on-path attackers to gain access to user credentials.

v3.1	**v4.0 Base**
5.9	8.2
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CVSS v4 Score: Base 8.2

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	Present	An attacker must be on-path to be able to intercept communications between affected systems.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.

Vulnerable System Confidentiality	High	An attacker could access plain text user credentials.
Vulnerable System Integrity	None	There is no impact to the vulnerable system integrity.
Vulnerable System Availability	None	There is no impact to the vulnerable system availability.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.

Denial of Service – **CVE-2023-22394**

Description
Memory leak due to receipt of specially crafted SIP calls (CVE-2023-22394)
An Improper Handling of Unexpected Data Type vulnerability in the handling of SIP calls in Junos OS on SRX Series and MX Series platforms allows an attacker to cause a memory leak leading to Denial of Services (DoS).

	v3.1	**v4.0**
Base	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	8.7 CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L
Base + Threat		6.6 CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L/E:U

CVSS v4 Score: Base + Threat 6.6

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	None	There is no impact to the vulnerable system confidentiality.
Vulnerable System Integrity	None	There is no impact to the vulnerable system integrity.
Vulnerable System Availability	High	An **Improper Handling of Unexpected Data Type** vulnerability in the handling of SIP calls in Juniper Networks Junos OS on SRX Series and MX Series platforms allows an attacker to cause a memory leak leading to denial of service.
Subsequent System Confidentiality	None	There is no confidentiality impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to the integrity of subsequent systems.
Subsequent System Availability	Low	The subsequent device could be unavailable/unreachable for a brief period of time.
Exploit Maturity	Unreported	There is no known proof-of-concept or malicious exploitation of this vulnerability.

Cross-Site Scripting (Reflected) – **CVE-2022-24682**

Categories: XSS

An issue was discovered in the Calendar feature in Zimbra Collaboration Suite 8.8.x before 8.8.15 patch 30 (update 1), as exploited in the wild starting in December 2021. An attacker could place HTML containing executable JavaScript inside element attributes. This markup becomes unescaped, causing arbitrary markup to be injected into the document.

v3.1	**v4.0 Base**
6.1	5.1
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

CVSS v4 Score: Base 5.1

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	Active	A targeted user must click a malicious link that is provided by an attacker.
Vulnerable System Confidentiality	None	There is no direct impact to the web application confidentiality.
Vulnerable System Integrity	None	There is no direct impact to the web application integrity.
Vulnerable System Availability	None	There is no direct impact to the web application availability.
Subsequent System Confidentiality	Low	An attacker could read data from the user's browser.

Subsequent System Integrity	Low	An attacker could modify data in the user's browser.
Subsequent System Availability	None	There is no direct availability impact to the user's browser.

Cross-Site Scripting (Stored) – **CVE-2020-0926**

Microsoft Office SharePoint XSS Vulnerability

Description
A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'.

An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.

v3.1	**v4.0 Base**
5.4	5.1
CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

CVSS v4 Score: Base 5.1

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.

Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	Low	The attacker requires privileges sufficient to store data within the application.
User Interaction	Passive	A targeted user must browse to the application as part of normal operations.
Vulnerable System Confidentiality	None	There is no direct impact to the web application confidentiality.
Vulnerable System Integrity	None	There is no direct impact to the web application integrity.
Vulnerable System Availability	None	There is no direct impact to the web application availability.
Subsequent System Confidentiality	Low	An attacker can read content that the attacker is not authorized to read from the user's browser.
Subsequent System Integrity	Low	An attacker could inject malicious content that could be executed within the user’s browser.
Subsequent System Availability	None	There is no direct impact to the user’s browser availability.

Privilege Escalation (Unprivileged) **CVE-2022-20759**

Description

Cisco Adaptive Security Appliance Firepower Threat Defense (FTD) Privilege Escalation Vulnerability (CVE-2022-20759)

A vulnerability in the web services interface for remote access VPN features of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, but unprivileged, remote attacker to elevate privileges to level 15.

An attacker could exploit this vulnerability by sending crafted HTTPS messages to the web services interface of an affected device. A successful exploit could allow the attacker to gain privilege level 15 access to the web management interface of the device.

v3.1	v4.0 Base
8.8	7.7
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVSS v4 Score: Base 7.7

Metric	Value	Comments
Attack Vector	Network	Attacks are executed through HTTPS requests.
Attack Complexity	Low	No advanced knowledge is required
Attack Requirements	Present	HTTP Management Access *and* IKEv2 Client Service must be enabled on at least one interface, or HTTP management interface *and* WebVPN must be enabled on at least one interface.
Privileges Required	Low	An attacker must have valid credentials for the VPN.
User Interaction	None	No additional user interaction is required for successful exploitation.
Vulnerable System Confidentiality	High	Successful exploitation could result in a complete compromise (enable 15) of the targeted device, which results in a complete (High) impact on the confidentiality of the device.
Vulnerable System Integrity	High	Successful exploitation could result in a complete compromise resulting in High integrity impact.
Vulnerable System Availability	High	Successful exploitation could result in a complete compromise resulting in High availability impact.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.

Privilege Escalation (Highly Privileged) **CVE-2021-34724**

Description

A vulnerability in the Cisco IOS XE SD-WAN Software CLI could allow an authenticated, local attacker to elevate privileges and execute arbitrary code on the underlying operating system as the root user. An attacker must be authenticated on an affected device as a PRIV15 administrative user.

	v3.1	**v4.0**
Base	6.0 CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N	8.3 CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N
Base + Threat		5.6 CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U

CVSS v4 Score: Base + Threat 5.6

Metric	Value	Comments
Attack Vector	Local	An attacker must be able to access the vulnerable system with a local, interactive session.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	High	An attacker must have administrator privileges within the affected system.
User Interaction	None	No additional user interaction is required for exploit

Vulnerable System Confidentiality	High	An attacker could execute arbitrary commands on the affected system with the privileges of the *root* user, allowing the privileged attacker to access sensitive files that would otherwise be inaccessible to the administrative user.
Vulnerable System Integrity	High	An attacker could execute arbitrary commands on the affected system with the privileges of the *root* user, allowing the privileged attacker to modify system values that would otherwise be inaccessible to the administrative user.
Vulnerable System Availability	None	An attacker does not gain any additional privileges to impact system availability. Privileges required to exploit this vulnerability already allow the attacker to turn off the system, so there is no privilege gain as a result of exploitation.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.
Exploit Maturity	Unreported	There is no known proof-of-concept code or malicious exploitation of this vulnerability.

Remote Code Execution (**CVE-2023-28311**)

Microsoft Word Remote Code Execution Vulnerability

An attacker must send the user a malicious file and convince the user to open said file which results in RCE.

v3.1	**v4.0 Base**
7.8	8.5

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVSS v4 Score: Base 8.5

Metric	Value	Comments
Attack Vector	Local	The document must be present on the local disk.
Attack Complexity	Low	Nothing outside of the attacker's control.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	Passive	A user must open a document.
Vulnerable System Confidentiality	High	The attacker could execute arbitrary code, which could allow the attacker to compromise the affected system completely.
Vulnerable System Integrity	High	The attacker could execute arbitrary code, which could allow the attacker to compromise the affected system completely.
Vulnerable System Availability	High	The attacker could execute arbitrary code, which could allow the attacker to compromise the affected system completely.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.

Arbitrary Code Execution **CVE-2022-22965**

Spring4shell

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

Attack

An RCE can be established by simply sending a series of malicious web requests to a web server running on a vulnerable version of Spring. Spring4Shell allows attackers to get arbitrary code execution in the context of the user that is running the vulnerable application. Once the attackers achieve RCE, they can install malware or can use the server as an initial foothold to escalate privileges and compromise the whole system, or even access subsequent backend systems that the vulnerable server has privileged access to.

v3.1	**v4.0 Base + Threat**
9.8	9.2
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A

CVSS v4 Score: Base + Threat 9.2

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	Present	A successful attack depends on the deployment and execution conditions of the vulnerable system.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	The vulnerability allows an attacker to execute arbitrary code in the context of the user that is running the

		vulnerable application and gain complete control over the system.
Vulnerable System Integrity	High	The vulnerability allows an attacker to execute arbitrary code in the context of the user that is running the vulnerable application and gain complete control over the system.
Vulnerable System Availability	High	The vulnerability allows an attacker to execute arbitrary code in the context of the user that is running the vulnerable application and gain complete control over the system.
Subsequent System Confidentiality	None	There is no immediate loss of confidentiality within the subsequent systems. But, based on how Spring is deployed in the target environment, the compromised server could be used as a pivot to leverage further. If there are subsequent impacts, they should be defined in environmental metrics.
Subsequent System Integrity	None	There is no immediate loss of integrity within the subsequent systems. But, based on how Spring is deployed in the target environment, the compromised server could be used as a pivot to leverage further. If there are subsequent impacts, they should be defined in environmental metrics.
Subsequent System Availability	None	There is no immediate loss of availability within the subsequent system. But, based on how Spring is deployed in the target environment, the compromised server could be used as a pivot to leverage further. If there are subsequent impacts, they should be defined in environmental metrics.
Exploit Maturity	Attacked	There are known exploits in the wild.

Physical Access **(CVE-2022-20826)**

A vulnerability in the secure boot implementation of Cisco Secure Firewalls 3100 Series that are running Cisco Adaptive Security Appliance (ASA) Software or Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated attacker with physical access to the device to bypass the secure boot functionality. This vulnerability is due to a logic error in the boot process. An attacker could exploit this vulnerability by injecting malicious code into a

specific memory location during the boot process of an affected device. A successful exploit could allow the attacker to execute persistent code at boot time and break the chain of trust.

v3.1	**v4.0 Base**
6.4	5.4
CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVSS v4 Score: Base 5.4

Metric	Value	Comments
Attack Vector	Physical	An attacker requires physical access to a vulnerable system.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	Present	There are timing requirements outside the attacker's control, making exploit attempts unreliable.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	An attacker could inject malicious, unsigned code and execute arbitrary commands.
Vulnerable System Integrity	High	An attacker could inject malicious, unsigned code and execute arbitrary commands.
Vulnerable System Availability	High	An attacker could inject malicious, unsigned code and execute arbitrary commands.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.

Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.

Information Disclosure – **CVE-2022-21500**

Description

Vulnerability in Oracle E-Business Suite (component: Manage Proxies). The supported version that is affected is 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle E-Business Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle E-Business Suite accessible data.

Note: Authentication is required for successful attack, however the user may be self-registered. Oracle E-Business Suite 12.1 is not impacted by this vulnerability. Customers should refer to the Patch Availability Document for details.

v3.1	**v4.0 Base**
7.5	8.7
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CVSS v4 Score: Base 8.7

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.

Vulnerable System Confidentiality	High	An attacker could exploit the vulnerability to access critical data that is stored within the vulnerable application.
Vulnerable System Integrity	None	There is no impact to the vulnerable system integrity.
Vulnerable System Availability	None	There is no impact to the vulnerable system availability.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.

Information Disclosure - **CVE-2021-32570**

In Ericsson Network Manager (ENM) releases before 21.2, users belonging to the same AMOS authorization group can retrieve the data from certain log files. All AMOS users are considered to be highly privileged users in the ENM system and all must be previously defined and authorized by the Security Administrator. Those users can access some log's files, under a common path, and read information stored in the log's files in order to conduct privilege escalation.

v3.1	**v4.0 Base**
4.9	6.9
CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CVSS v4 Score: Base 6.9

Metric	Value	Comments

Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	High	An attacker must have membership in the AMOS authorization group sufficient to read data from log files.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	An attacker could exploit the vulnerability to view sensitive data within the application log files.
Vulnerable System Integrity	None	There is no impact to the vulnerable system integrity.
Vulnerable System Availability	None	There is no impact to the vulnerable system availability.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.

Command Injection (**CVE-2022-26134**)

Description

Atlassian Confluence Server and Data Center OGNL Injection Vulnerability (CVE-2022-26134)

In Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance.

A remote attacker could exploit it by requests injecting specially crafted OGNL templates in order to execute arbitrary code.

v3.1	**v4.0 Base**

9.8	9.3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVSS v4 Score: Base 9.3

Metric	Value	Comments
Attack Vector	Network	Attacks are executed through HTTP(s) requests and are accessible from remote networks.
Attack Complexity	Low	No advanced knowledge is required
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	Successful exploitation could result in a complete compromise (command execution as *root*) of the affected device, which results in a complete (High) impact on the confidentiality of the device.
Vulnerable System Integrity	High	Successful exploitation could result in a complete compromise (command execution as *root*) of the affected device, which results in a complete (High) impact on the integrity of the device.
Vulnerable System Availability	High	Successful exploitation could result in a complete compromise (command execution as *root*) of the affected device, which results in a complete (High) impact on the availability of the device.
Subsequent System Confidentiality	None	There are no additional impacts to subsequent systems.
Subsequent System Integrity	None	There are no additional impacts to subsequent systems.
Subsequent System	None	There are no additional impacts to subsequent systems.

Availability		

Industrial Control Systems (ICS) (**CVE-2023-28728**)

Description:

In Panasonic Control FPWIN versions 7.6.0.3 and prior, a stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or a parameter to a function) when a file is opened within the application.

v3.1	**v4.0**
7.8	8.5
CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:P

CVSS v4 Score: Base 8.5

Metric	Value	Comments
Attack Vector	Local	An attacker must be locally connected to the vulnerable system.
Attack Complexity	Low	No built-in security-enhancing conditions exist within the product to inhibit successful exploitation.
Attack Requirements	None	The attacker can execute the exploit with no specific difficulty. No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	Passive	A user, other than the attacker, must be present for the vulnerability to be exploited. However, the actions taken by the user are typical, because a user must open a file within the vulnerable application.
Vulnerable System Confidentiality	High	Exploitation of the vulnerability results in complete control of the vulnerable system.

Vulnerable System Integrity	High	Exploitation of the vulnerability results in complete control of the vulnerable system.
Vulnerable System Availability	High	Exploitation of the vulnerability results in complete control of the vulnerable system.
Subsequent System Confidentiality	None	The impact on confidentiality is limited to the vulnerable system. No direct downstream impact is indicated.
Subsequent System Integrity	None	The impact on integrity is limited to the vulnerable system. No direct downstream impact is indicated.
Subsequent System Availability	None	The impact on availability is limited to the vulnerable system. No direct downstream impact is indicated.
Safety	Present	The impact from an attacker gaining full control of software that is running on a programmable logic controller (PLC) may meet the definition of IEC 61508 consequence category **marginal**, **critical** or **catastrophic** for certain usage of the PLC in an Operational Technology (OT) environment where humans may be harmed.

IOT - Healthcare (**CVE-2020-10627**)

Description:

Insulet Omnipod Insulin Management System insulin pump product ID 19191 and 40160 is designed to communicate using a wireless RF with an Insulet manufactured Personal Diabetes Manager device. This wireless RF communication protocol does not properly implement authentication or authorization. An attacker with access to one of the affected insulin pump models may be able to modify and/or intercept data. This vulnerability could also allow attackers to change pump settings and control insulin delivery.

	v3.1	**v4.0**
Base	8.1 CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	8.6 CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/S:P
Base + Environmental		9.7

		CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/MSI:S/S:P

CVSS v4 Score: Base + Environmental 9.7

Metric	Value	Comments
Attack Vector	Adjacent	An attacker must be within the local proximity of the device.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No attack requirements are present.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	An attacker could exploit the vulnerability to intercept critical data.
Vulnerable System Integrity	High	An attacker could exploit the vulnerability to change pump settings and control insulin delivery.
Vulnerable System Availability	None	There is no impact to the vulnerable system availability.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.
Exploit Maturity	Unreported	There is no known proof-of-concept code or malicious exploitation of this vulnerability.
Modified Subsequent System	Safety	Because control of insulin delivery can be changed, there is a health and human safety impact.

Safety	Present	Impact on health and human safety from a vulnerability in an OT device may meet definition of IEC 61508 consequence category **critical**.

Value Density (**CVE-2020-28196**)

Description:

MIT Kerberos 5 (aka krb5) before 1.17.2 and 1.18.x before 1.18.3 allows unbounded recursion via an ASN.1-encoded Kerberos message because the lib/krb5/asn.1/asn1_encode.c support for BER indefinite lengths lacks a recursion limit.

	v3.1	**v4.0 Base**
Base	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	8.7 CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/V:C

CVSS v4 Score: Base 8.7

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No attack requirements are present.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	None	There is no impact to the vulnerable system confidentiality.
Vulnerable System Integrity	None	There is no impact to the vulnerable system integrity.
Vulnerable System	High	An attacker could cause the application to fail and restart,

Availability		resulting in a denial of service condition.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.
Value Density	Concentrated	The value of the Kerberos system is highly concentrated due to its functionality in the network environment.

Version History

2023-08-10	v0.1	Initial Publication
2023-09-29	v0.2	Grammatical editing changes, updated metrics score comments, and corrected metric score mismatches. Updated CVE-2021-44228
2023-10-30	v0.3	Added new examples for Value Density (CVE-2020-28196) and Safety (CVE-2023-30560). Additional error corrections
2023-11-01	v1.0	Official Release