Collecting PSIRT Metrics That Drive Change

Steve Hart, CISSP, CCSP
Head of Product Security, Research and Development

Sallie Newton, CISSP, PCI-P, GISP
PSIRT Lead, Research and Development

Brian English
Product Security Lead, Technical Support
About SAS Institute
40+ years of analytics innovation

Solutions

› Advanced Analytics
› AI Solutions
› Business Intelligence & Analytics
› SAS & Cloud Computing
› Customer Intelligence
› Data Management
› Decision Management
› Fraud & Security Intelligence
› Solutions for Hadoop
› IoT Analytics Solutions
› Performance Management
› Personal Data Protection
› Risk Management
› Supply Chain Intelligence

Company Facts & Financials

<table>
<thead>
<tr>
<th>Customer</th>
<th>Employee</th>
<th>Financial</th>
</tr>
</thead>
</table>
| **Number of Countries Installed**
SAS has customers in 147 countries. | **Worldwide Employees**
13,939 total employees | **Worldwide Revenue**
2018 Revenue: US$3.27 billion
Historical revenue data |
| **Total Worldwide Customer Sites**
Our software is installed at more than 83,000 business, government and university sites. | **Breakdown by Geography**
United States: 6,908
World Headquarters (Cary, NC): 5,545
Canada: 312
Latin America: 491
Europe, Middle East and Africa: 3,592
Asia Pacific: 2,601 | **Reinvestment in R&D**
2018 R&D investment: 26% of revenue |
| **Fortune Global 1000® Customers**
92 of the top 100 companies on the 2018 Fortune Global 1000® are SAS customers. |
Agenda

1. Establishing a PSIRT at SAS Institute
2. PSIRT Metrics in Research and Development
3. PSIRT Metrics in Customer Support
Establishing a PSIRT at SAS Institute

Steve Hart, CISSP, CCSP
Head of Product Security, Research and Development
What’s happening in the industry around this same timeframe that could be driving all of this activity?
Establishing PSIRT at SAS Institute

Phase 1

• 2016

  • Reactive -> Proactive
  • Establish a framework for how to operate
  • Organize around industry standards, best practices and guidelines
    • FIRST
    • CWE
    • CVE
    • CVSS
    • OWASP
    • NIST
    • BSIMM
    • SAMM

Source: https://owasp.org/www-project-samm/
Establishing PSIRT at SAS Institute

Phase 2

• 2017
  • Implementation of a Software Security Program
  • Roll out security tooling and guidance
  • Establish Security Champions
  • Shift Left

Security Activities within the Software Development Life Cycle (SDLC)
Establishing PSIRT at SAS Institute

Phase 3

• 2018
  • 100% participation across Research & Development
  • Streamlined process
  • Collection of security artifacts tracked in project level security reviews
Establishing PSIRT at SAS Institute
Phase 4

• 2019-2020
  • Maturing and optimizing security practices
    • security architecture design review
    • secure coding developer guidance
    • internal penetration testing
    • root cause analysis
  • Automation - go faster to support CI/CD and shorten PSIRT remediation timelines
  • Expand scope to cover new technologies (Cloud-Native, Containers, K8s)
  • Build security culture
    • security open forums
    • cybersecurity month activities
    • revamp security champions program

PSIRT Metrics from Research and Development

Sallie Newton, CISSP, PCI-P, GISP
PSIRT Lead, Research and Development
PSIRT Metrics from R&D

There are 5 phases to our PSIRT process:

• Vulnerability Discovery
• Vulnerability Triage
• Vulnerability Remediation
• Vulnerability Disclosure
• Post-Incident Review  A.K.A  LESSONS LEARNED
What are metrics?

a method of measuring something
PSIRT Metrics from R&D

Why metrics matter?
PSIRT Metrics from R&D

ISO | NIST | GDPR | FedRAMP | Enterprise | FIPS
PSIRT Metrics from R&D
PSIRT Metrics from R&D

What to measure
PSIRT Metrics from R&D

Threat Modeling Metrics
PSIRT Metrics from R&D

Vulnerability Discovery

Internal
External
PSIRT Metrics from R&D

Mitigation: Patches vs Next Release

To Patch, Or Not To Patch
THAT IS THE QUESTION!
Types of Vulnerabilities

PSIRT Metrics from R&D
PSIRT Metrics from R&D

SAS Top Five OWASP Vulnerabilities

OWASP Top 10
PSIRT Metrics from R&D

OWASP Top 10 Vulnerabilities

OWASP Top 10 - 2017

A1: 2017-Injection
A2: 2017-Broken Authentication
A3: 2017-Sensitive Data Exposure
A4: 2017-XML External Entities (XXE) [NEW]
A5: 2017-Broken Access Control [Merged]
A6: 2017-Security Misconfiguration
A7: 2017-Cross-Site Scripting (XSS)
A8: 2017-Insecure Deserialization [NEW, Community]
A9: 2017-Using Components with Known Vulnerabilities
A10: 2017-Insufficient Logging & Monitoring [NEW, Comm.]
PSIRT Metrics from R&D

SAS Top 10 - 2019

- Broken Access Control
- XSS
- Injection
- Misconfiguration
- Sensitive Data Exposure
- Using Components w/known vulnerabilities
- Broken Authentication
- Insecure Deserialization
### SAS Top 10 - 2019

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>A9:2019 - Using Components w/known vulnerabilities</td>
</tr>
<tr>
<td>13</td>
<td>A5: 2019 - Broken Access Control</td>
</tr>
<tr>
<td>11</td>
<td>A7:2019 - XSS</td>
</tr>
<tr>
<td>7</td>
<td>A2:2019 - Broken Authentication</td>
</tr>
<tr>
<td>7</td>
<td>Other (None OWASP Top 10)</td>
</tr>
<tr>
<td>6</td>
<td>A1:2019 - Injection</td>
</tr>
<tr>
<td>3</td>
<td>A3:2019 - Sensitive Data Exposure</td>
</tr>
<tr>
<td>2</td>
<td>A8:2019 - Insecure Deserialization</td>
</tr>
<tr>
<td>1</td>
<td>A6:2019 - Misconfiguration</td>
</tr>
</tbody>
</table>

Product Vulnerabilities Prioritized by Frequency
Total 55 of 68 = 81% of our vulnerabilities reside in 5 domains

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>A9:2019 - Using Components w/known vulnerabilities</td>
</tr>
<tr>
<td>13</td>
<td>A5: 2019 - Broken Access Control</td>
</tr>
<tr>
<td>11</td>
<td>A7:2019 - XSS</td>
</tr>
<tr>
<td>7</td>
<td>A2:2019 - Broken Authentication</td>
</tr>
<tr>
<td>6</td>
<td>A1:2019 - Injection</td>
</tr>
</tbody>
</table>
PSIRT Metrics from R&D

Training, Awareness & Education
PSIRT Metrics from R&D
PSIRT Metrics from R&D

### SAS Top 5 - Training Domains

<table>
<thead>
<tr>
<th>Training Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. A9:2019 - Using Components w/known vulnerabilities</td>
</tr>
<tr>
<td>2. A5: 2019 - Broken Access Control</td>
</tr>
<tr>
<td>3. A7:2019 - XSS</td>
</tr>
</tbody>
</table>
PSIRT Metrics from R&D

Guidance - Top Five Testing Recommendations

<table>
<thead>
<tr>
<th>SAS Top 5 - Testing Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>
PSIRT Metrics from R&D

Support Security and Compliance Decisions with Metrics
PSIRT Metrics from Customer Support

Brian English
Product Security Lead, Technical Support
PSIRT Metrics from Customer Support

What can be learned from Customer Support Data?

• Measure cost and manpower required to address customer reported security vulnerabilities.

• Scope PSIRT staffing needs in both customer support and R&D.

• Identify security metrics by
  • Customer
  • Country
  • Software release
  • Software products/solutions

• Identify pace of incoming security tracks vs. outgoing security patches.
PSIRT Metrics in Customer Support
Collecting Customer Support Data

- Ticket metadata added to identify security inquiries and incidents
- Other metadata allows granular reporting on issues
PSIRT Metrics in Customer Support

Interpreting Customer Support data

- Values represent number of customer inquiries, not necessarily product vulnerabilities.
- Broken out by year/quarter.
- Separated into tables featuring Customer Name, Country, Product Release, and Top Products.
• Identify customers and sectors most concerned about product security, or most active in security auditing
• Valuable to Sales/Marketing and Product Management
PSIRT Metrics in Customer Support
Interpreting Customer Support data

- Track workload for Customer Support in various regions
- Identify possible staffing needs
PSIRT Metrics in Customer Support
Interpreting Customer Support data

- Customers staying on old software versions
- More vulnerabilities in older versions
- Fewer vulnerabilities in new versions
PSIRT Metrics in Customer Support
Interpreting Customer Support data

- Products and components commonly targeted by scans (Apache, OpenSSL)
- Products that encompass many components
- Specific products that are targeted to certain customer sectors
- Products that simply have more vulnerabilities
PSIRT Metrics in Customer Support
What do customer reported problems mean for R&D?

• Identify resources and cost associated with Product Security fixes
• Establish association between customer inquiries and bug fixes

<table>
<thead>
<tr>
<th>Q1 2020 Summary: 12 Hot Fixes released addressing 15 Security Defects (10 unique)</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 2020 - 5 Hot Fixes released addressing 8 Security Defects (6 unique)</td>
</tr>
<tr>
<td>F1E007 02 / 25 / 20 Base SAS 9.4_M6 (18w47) S1516964 - SAS/Share libname third</td>
</tr>
<tr>
<td>V1a 02 / 21 / 20 S1455702 - CRP: Stored XSS via Data极力</td>
</tr>
<tr>
<td>C2L008 02 / 21 / 20 SAS Studio 3.71 (17w47) S1557661 - CRP: XSS in signout.jsp</td>
</tr>
<tr>
<td>V1a 02 / 18 / 20 SAS Viya 3.5 for Linux S1558010 - CRP: Viola exploit mitigated in</td>
</tr>
<tr>
<td>D8F004 02 / 10 / 20 SAS Studio 3.8 (18w47) S1520172 - CRP: SASGraphBuilder</td>
</tr>
<tr>
<td>January 2020 - 7 Hot Fixes released addressing 7 Security Defects (4 unique)</td>
</tr>
<tr>
<td>F6R002 01 / 30 / 20 SAS Fraud Management 6.1 (19w25) S1554388 - CRP: XSS in the Alert</td>
</tr>
<tr>
<td>D9T067 01 / 30 / 20 Base SAS 9.4_M6 (19w47) S1548101 - CRP PERFORMANCE: Higher</td>
</tr>
<tr>
<td>B6T011 01 / 22 / 20 SAS Management Console 9.4_M5 (17w38) S15542451 - CRP: Communications</td>
</tr>
</tbody>
</table>
PSIRT Metrics in Customer Support

What Next?

• The missing link... bridge the gap between the customer tracking system and our R&D defects/jira system.

• As we upgrade or transition to new tools, ensure data model improvements are considered in the design to aid the collection and quality of metrics.
Driving Change
What did we learn from all this?

1. Start with tracking security defects
2. Score all security defects honestly
3. Use a well known maturity model to help guide you (e.g. SAMM)
4. Identify trends and patterns in your PSIRT data
5. Prioritize, you can’t fix everything all at once
6. Utilize free resources for vulnerability data (e.g. NVD, OWASP)
7. Let security tools do some of the heavy lifting (e.g. SAST, DAST, SCA)
8. Threat Modeling can be very powerful once understood
9. Continuous professional education is extremely important
10. Regular update meetings with leadership (e.g. quarterly)
Questions