SAP Bug Bounty Program for SAP S/4HANA

Patrick Boch, Product Manager SAP S/4HANA Security, SAP SE
Ravishankar Sahadevan, Global Lead S/4HANA Bug Bounty & COO S/4HANA Security, SAP SE
July 21st, 2022
The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP’s strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.
Agenda

The Security of SAP S/4HANA

What is Bug Bounty?

Why Bug Bounty?

Where to report security issues to SAP?

Bug Bounty @S/4HANA
The Security of SAP S/4HANA
Confidence in SAP S/4HANA Security through a holistic approach

Security is integrated into SAP Company Processes

- Risk based approach aligned to ISO 27034
- Threat modelling
- Code scans
- Data Protection & Privacy assessment (DPCE)
- Internal & external security assessment

- Continuous security fixes and enhancements
- SAP S/4HANA Bug Bounty Program
- Digitally signed code
- Security validation

Secure Cloud Software Development

Leading Security and DPP Products & Features

Secure Operations & Landscape Architecture

Security Products
SAP Secure Software Development and Operations Lifecycle
From Risk Assessment to Security Validation

The Secure Software Development and Operations Lifecycle is the framework at SAP to develop software that fulfills both Security and Data Protection & Privacy requirements.

SAP follows a risk-based approach to efficiently achieve security within economic boundaries:
- Product teams first identify security risks by conducting security risk assessments
- Performing security activities to embed security in the product and verify its effectiveness for the identified risks

<table>
<thead>
<tr>
<th>Preparation</th>
<th>Development</th>
<th>Transition</th>
<th>Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security awareness</td>
<td>Plan Security features</td>
<td>Independent security assessment</td>
<td>Bug Bounty</td>
</tr>
<tr>
<td>Secure programming</td>
<td>Secure Development</td>
<td>Independent data protection and privacy assessment</td>
<td>Incident Management</td>
</tr>
<tr>
<td>Threat modeling</td>
<td>Secure programming</td>
<td>Automated security testing</td>
<td></td>
</tr>
<tr>
<td>Product Standard Assessment</td>
<td>Security code scan</td>
<td>Manual internal and external security assessment</td>
<td></td>
</tr>
<tr>
<td>Data Protection Compliance Evaluation</td>
<td>Open source vulnerability scans</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Common denominator: Product standard security as knowledge base across all phases
What is Bug Bounty?
Bug bounty history and basics

"Crowdsourced Penetration Testing" - Ethical hackers are rewarded for finding vulnerabilities

- Strict rules for what is in scope and what is out
- Responsible disclosure of findings
- Rewards (bounties) are paid according to criticality of the finding based on CVSS (Common Vulnerability Scoring System)
Why Bug Bounty?
Offensive Security Testing

Penetration Tests

Hacking Simulations
(Red Team)

Bug Bounty
SAP’s journey to bug bounty program

2016
Public “Hall of Fame” for security researchers submitting vulnerabilities to SAP Secure Inbox

2017 - 2021
Set up and continuous evolution of bug bounty programs at SAP

2022 onwards
General availability of bug bounty programs for all interested applications at SAP

- One of the main sources for vulnerability findings beside general vulnerability reports and customer disclosures
- 75% true positive rate
- 17% of disclosures rated with CVSS higher than 7.0
- Reward range between $100 and $4000 to submissions with CVSS scores between 2.9 and 9.6
- Average payout $983 per vulnerability
- Findings range from simple vulnerabilities to design flaws
Bug Bounty vs Conventional Security Testing

**Bug Bounty**
- After product release
- Defined scope (in / out of scope definition)
- Ongoing
- As many testers as you like
- Regular scope extensions
- Private and public programs
  - *Private*: Invited hackers only
  - *Public*: All hackers who are registered with the bug bounty platform service provider

**Conventional security testing**
- During the development lifecycle of a product
- Narrow scope
- One time activity at a set point in time with limited pen testers

Bug Bounty in the Secure Software Development and Operations Lifecycle

- **Preparation**
  - Training
  - Risk Assessment

- **Development**
  - Plan Security Measures
  - Secure Development
  - Security Testing

- **Transition**
  - Security Validation

- **Utilization**
  - Bug Bounty
Where to report security issues to SAP?
Product Security Findings

Report a Security Issue

SAP is committed to identifying and addressing security issues that affect our software and cloud solutions. We are continuously working on improving our security processes. To report a potential security issue, choose from the options below.

SAP customers
Report a customer security issue by using the SAP ONE Support Launchpad to find a solution and get real-time support from an expert.
View the launchpad

Security researchers
Inform the SAP Security Response Team of a security issue by completing and submitting the security vulnerability form.
Access the form

Note: Include the following details in the report, as applicable, so that we can better analyze the nature and scope of the security issue: issue category, affected product version with support package and patch level, necessary pre/post-conditions for the exploit to work, description with proof of concept or exploit code, and impact of the issue if exploited.

https://www.sap.com/about/trust-center/security/incident-management.html

© 2022 SAP SE or an SAP affiliate company. All rights reserved. | Public
SAP Security Patch Day and Researcher Acknowledgement

SAP Security Patch Day

Fix vulnerabilities discovered in SAP products
Review notes from our monthly SAP Security Patch Day to learn about vulnerabilities discovered in SAP products and apply patches to protect your SAP landscape.

Read the SAP Security Patch Day blog

Join us in acknowledging our security researchers
Learn about the security researchers who help us identify and solve security vulnerabilities, so we can help maintain the security and safety of our customers and partners.

See the list of security researchers

SAP Trust Center – Security – Security Issue Management
Bug Bounty @ S/4HANA
SAP S/4HANA Bug Bounty Program – Overview

Goal

To establish an **external security verification platform** for S/4HANA to **financially incentivize** responsible disclosure by external security researchers and **leverage** synergy of **crowdsourced security testing**

Advantage

**Continuous** external security verification post **General Availability (GA)** of S/4HANA with **high external visibility**. Reported findings **improve the security of S/4HANA (On Premise & Cloud)**

Collaboration

Launched through **SGS Bug Bounty Service** and **Operated by BugBounty Platform Provider**

Bug Bounty
SAP S/4HANA Bug Bounty Program – Focus On-Premise

Systems
- S/4HANA On-Premise is used based on the Fully Activated Appliance from SAP Cloud Appliance Library (CAL), e.g. [https://cal.sap.com/catalog#/solutions/a0b63a18-0fd3-4d88-bbb9-4f02c13dc343](https://cal.sap.com/catalog#/solutions/a0b63a18-0fd3-4d88-bbb9-4f02c13dc343)

Scope
- First release in 2019
  - S/4HANA On-Premise 1809 FPS01 with activated functional scope: SAP Finance
- Second release in 2020
  - S/4HANA On-Premise 1909 FPS02 with activated functional scope: SAP Finance and SAP Transport Mgmt
- Current release in 2022
  - S/4HANA On-Premise 2020 FPS01 with activated functional scope: SAP Finance, SAP Transport Mgmt, Logistics & Sales and Distribution
SAP S/4HANA Bug Bounty Program – Focus Cloud

Systems
- S/4HANA Cloud is an isolated tenant in the production landscape based on the S/4HANA Cloud Starter Edition

Scope
- First release in 2022 (S/4HANA Cloud 2202) with selected scope in certain areas
  - Accounts Payable
  - General Ledger
  - Master Data
  - Post Goods Movement
SAP S/4HANA Bug Bounty Program – Highlights & Challenges

**Highlights**

- High value findings (P1 & P2)

- **42** Total submissions
- **$~1900** Average reward
- **400+** Security researchers
- **72%** True positive rate

**Standard Reward Ranges**

- P1: $(4000-5000)
- P2: $(2000-3500)
- P3: $(1500-700)
- P4: $(500-250)

**Promotional Reward Ranges (Live-S/4H OP)**

- P1: $(6000-8000)
- P2: $(4000-5000)
- P3: $(1000-2000)
- P4: $(350-600)

**Challenges**

- Tailored Application scope
- Test-Data for the applications
- Managing / Verifying hardening for every layer (Application, Platform, DB, OS, IaaS)
- Compliance to SAP Global Security checklist
- Regular Maintenance & Monitoring
- Budget for Bug Bounty
- Managing continuous traction
- Sustaining the Bug Bounty program
- Running a bounty service for S/4HANA On-Premise
Learnings

- **Start with small scope** & plan for fill scope enablement via roadmap
- **Invest in application knowledge**
- Managing **continuous traction** via onboarding researches, scope, enhancements, reward structure
- **High True positive** rates of findings
- Researches provide **new vulnerability patterns / ideas**

Vulnerability Analysis

- **56%** Denial of Service
- **7%** Information Disclosure
- **7%** Missing Authorization Check
- **4%** Missing XML Validation
- **19%** Other
- **4%** URL Redirection
- **4%** Cross Site Scripting
SAP S/4HANA Bug Bounty Program – Roadmap

**Incubation**
- Scope aligned
- Pilot planned
- SGS Co-sponsor
- Budget Secured

**2018**
- S/4H BB team formed
- S/4HANA On-Premise 1809
- Scope: Finance
- Go-Live Oct. 2019

**2019**
- Pilot
- S/4HANA On-Premise 1909 with Scope: Finance and TM

**2020**
- Findings across stack
- Upgrade: Q3 2020
- S/4HANA On-Premise 1909 with Scope: Finance and TM

**2021**
- Scale
- High Value Findings
- Upgrade Q3 / 2022
- S/4HANA On-Premise 2020 with enhanced scope

**2022**
- Cloud Focus
- Extend to S/4HANA Cloud
- Extend S/4HANA On-Premise to full scope
- Review reward

**2023**
- Public
- S/4HANA On-Premise target
- S/4HANA Cloud full scope

© 2022 SAP SE or an SAP affiliate company. All rights reserved. | Public
Thank you.

Contact information:

Patrick Boch
Product Management, S/4HANA Security
E-mail: patrick.boch@sap.com

Ravishankar Sahadevan
Global Lead S/4HANA Bug Bounty & COO
S/4HANA Security
E-mail: ravishankar.sahadevan@sap.com