The Truth Is Out There:
Mission-Critical SAP Applications Are Under Attack

JP Perez Etchegoyen, CTO, Onapsis
Discovered

800+
zero-day vulnerabilities in business-critical apps

Found

66%
of critical vulnerabilities
in Oracle EBS

Mitigated

60%
of SAP HANA unpatched vulnerabilities

3
US DHS critical alerts based on our research

50+
conference presentations

17
Patents

9
Patents Pending

8
Issued Patents

Featured In

REUTERS
WALL STREET JOURNAL
CNBC
Forbes
FORTUNE
A majority of organizations reported a breach of ERP systems in the past two years.
EVOLUTION OF MISSION-CRITICAL APPLICATION CYBERATTACKS

2012
- Hacktivist groups targeting SAP applications
- 1st public exploit targeting SAP applications discovered

2013
- Cyber criminals creating malware targeting SAP applications
- Chinese hacker exploits SAP NetWeaver

2014
- Public exploit

2015
- Nation-state sponsored
- Chinese breach of USIS targeted SAP

2016
- 1st DHS US-CERT Alert for SAP Business Applications
- Increased interest on dark web
- Onapsis helps Oracle secure critical vulnerability in EBS

2017
- 2nd DHS US-CERT Alert for SAP Business Applications

2018
- 3rd DHS US-CERT Alert for SAP 10KBLAZE Vulnerability

2019
- 4th DHS US-CERT Alert for SAP RECON Vulnerability
- Payday Oracle Vulnerabilities

2020
- Exploit toolkit
- SAP RFCpwn

2021
- Public exploit
- SAP SolMan
- 5th DHS US-CERT Alert on malicious activity targeting SAP applications

Onapsis Inc. | All Rights Reserved
Onapsis Inc. | All Rights Reserved

CONTEXT / MOTIVATION

ONAPSIS OFTEN ENGAGED FOR SAP INCIDENT RESPONSE SERVICES

• Over the last few years, Onapsis responded to several breaches affecting unprotected SAP applications that resulted in data theft, financial fraud and business disruption.

• Engagements strictly confidential. No public information disclosed.

CAPTURE IN-THE-WILD THREAT INTEL ON SAP ATTACKS TO KEEP DEFENDERS AHEAD

• How prevalent are SAP attacks?
• How sophisticated are the threat actors?
• Who are they?
• What are their targets/intentions?
• What are their capabilities and tactics?
• How can we stop them?

Enhance governance and improve overall security of mission-critical applications
VULNERABILITIES IN SAP APPLICATIONS
1. Exploitation of EEM
2. Exploitation of SMDagent
3. Lateral movement with SAP Control escalating to root privileges on entire SAP landscape

Remark:
A public exploit for 1. (CVE-2020-6207 has been released on 14.01.2021)
CHALLENGE | SAP® PATCH MANAGEMENT

Example | Black Hat USA 2020: P. Artuso & Y. Genuer (Onapsis)
Example | Black Hat USA 2020: P. Artuso & Y. Genuer (Onapsis)
Example | Black Hat USA 2020: P. Artuso & Y. Genuer (Onapsis)

RESULT:
Root on SAP landscape
SAP_ALL in all systems
Black Hat USA 2020: “An Unauthenticated Journey to Root”

Related SAP OSS Notes

- Patch 2902645  [https://launchpad.support.sap.com/#/notes/2902645](https://launchpad.support.sap.com/#/notes/2902645)
- Patch 2902456  [https://launchpad.support.sap.com/#/notes/2902456](https://launchpad.support.sap.com/#/notes/2902456)
- Patch 2890213  [https://launchpad.support.sap.com/#/notes/2890213](https://launchpad.support.sap.com/#/notes/2890213)
- Patch 2808158  [https://launchpad.support.sap.com/#/notes/2808158](https://launchpad.support.sap.com/#/notes/2808158)
- Patch 2823733  [https://launchpad.support.sap.com/#/notes/2823733](https://launchpad.support.sap.com/#/notes/2823733)
- Patch 2839864  [https://launchpad.support.sap.com/#/notes/2839864](https://launchpad.support.sap.com/#/notes/2839864)
- Patch 2849096  [https://launchpad.support.sap.com/#/notes/2849096](https://launchpad.support.sap.com/#/notes/2849096)
- Patch 2772266  [https://launchpad.support.sap.com/#/notes/2772266](https://launchpad.support.sap.com/#/notes/2772266)
- Patch 2738791  [https://launchpad.support.sap.com/#/notes/2738791](https://launchpad.support.sap.com/#/notes/2738791)
- Patch 2748699  [https://launchpad.support.sap.com/#/notes/2748699](https://launchpad.support.sap.com/#/notes/2748699)
- Patch 2845377  [https://launchpad.support.sap.com/#/notes/2845377](https://launchpad.support.sap.com/#/notes/2845377)
- Patch 2904933  [https://launchpad.support.sap.com/#/notes/2904933](https://launchpad.support.sap.com/#/notes/2904933)
<table>
<thead>
<tr>
<th>Misconfiguration</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP gateway</td>
<td>Full system compromise: Attacker can execute arbitrary OS commands as &lt;sidadm&gt; allowing him to access and modify the database or to install arbitrary transports</td>
</tr>
<tr>
<td>SAP message server</td>
<td>Full system compromise: An attacker can bypass the gateway ACL and perform the SAP gateway exploit (if both exploits are chained)</td>
</tr>
<tr>
<td>SAP standard passwords</td>
<td>Depends on the user account. If a standard user has SAP_ALL then the system can be fully compromised (e.g., DDIC, SAP*), for other users it depends on the assigned authorizations. Old systems might even have SAP_ALL to TMSADM assigned.</td>
</tr>
<tr>
<td>Old password hashes on SAP NetWeaver ABAP</td>
<td>Old password hashes are used and the password hashes are not properly secured. An attacker can access them and start a bruteforce attack using John-The-Ripper or Hashcat. Subsequently he can impersonate other users or admin accounts. If old password hashes are used, then typically all passwords are broken within days.</td>
</tr>
<tr>
<td>RFC callback</td>
<td>Allows executing remote enabled functions from an RFC caller with his authorizations</td>
</tr>
<tr>
<td>RFC upward connections</td>
<td>RFC connection from Dev to Prod with a high-privileged user account</td>
</tr>
<tr>
<td>Critical authorizations assigned &amp; SOD</td>
<td>In many cases: full system compromise (e.g. debug &amp; replace in production, S_RFC *, SQVI, SE16, SE17, SE37, etc.)</td>
</tr>
</tbody>
</table>
Vulnerability Demonstrations
NOVEL EVIDENCE OF SOPHISTICATED THREAT ACTORS ACTIVELY EXPLOITING SAP APPLICATIONS IN-THE-WILD

300+ CONFIRMED EXPLOITATIONS

107+ HANDS-ON ATTACKS

7 TRACKED THREAT VECTORS

18 UNIQUE COUNTRIES

Data based on direct observation of threat activity against OTIC, upon unmarked systems becoming online. Data is not based on exploitation on SAP customers’ environments. * geo location can be affected by VPS / TOR
Threat Intelligence Report

• Threat Actors actively targeting SAP Applications by exploiting critical vulnerabilities, chaining them and accessing business data.

• Using 8 threat vectors including 6 CVEs and 2 CWEs

• A successful compromise could impact confidentiality, integrity and availability of mission-critical SAP applications, including significant compliance impact.

• Highlighted by CISA: https://us-cert.cisa.gov/ncas/current-activity/2021/04/06/malicious-cyber-activity-targeting-critical-sap-applications

SMALL WINDOW TO DEFEND

Rapid patching and secure Cloud provisioning is critical

Data based on direct observation of threat activity against OTIC, upon unmarked systems becoming online. Data is not based on exploitation on SAP customers’ environments.
OBSERVED THREAT 1
RECON (CVE-2020-6287)

- CVSS v10 vulnerability reported by Onapsis to SAP (May ’20).
- SAP promptly developed and released patch in ~45 days (July ’20).
- Successful exploitation leads to creation of unauthorized Administrative user account in unprotected SAP system, bypassing all change management controls.
- Continuously being scanned for and exploited.
- Observed *hands-on-keyboard* activity on the exploited systems. Attackers accessing business data and demonstrating advanced capabilities, including *patching the SAP system post-exploitation.*
OBSERVED THREAT 2
SOLMAN (CVE-2020-6207)

• SolMan is the “Active Directory” of SAP.
• CVSS v10 vulnerability reported by Onapsis to SAP (Feb 2020).
• SAP promptly developed and released patch in ~30 days (Mar 2020).
• Successful exploitation leads to full control of SolMan and connected systems.
• On Jan 14th, 2021 a public exploit was released on GitHub.
• Significant scanning and exploitation activity followed.
• Onapsis captured evidence of related activity 3 months before exploit release.
• Evidence of attackers exploiting SAP vulnerabilities through private, undisclosed SAP exploits.
OBSERVED THREAT 3
PRIVILEGED SAP USER BRUTEFORCING (CWE-798)

- Active bruteforce was detected, using well-known technical accounts in SAP.
- If not properly secured, attackers could abuse system accounts with default passwords.
- Successful logins with these users leads to full compromise (SAP_ALL / Admin privileges) of all SAP business information and processes.
- SAP has provided secure configuration guidelines for this matter which should be implemented.

Protecting Standard Users

SAP\*, DDC, EARLYWATCH
SAP Systems create the standard users SAP\*, DDC and EARLYWATCH during the installation process in the clients as shown in the table below.

<table>
<thead>
<tr>
<th>User</th>
<th>Description</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP*</td>
<td>SAP system super user</td>
<td>000, 001, 066</td>
</tr>
<tr>
<td></td>
<td></td>
<td>all new clients</td>
</tr>
<tr>
<td>DDC</td>
<td>ABAP Dictionary and software logistics super user</td>
<td>000, 001</td>
</tr>
<tr>
<td>EARLYWATCH</td>
<td>Dialog user for the Early Watch service in client</td>
<td>066</td>
</tr>
</tbody>
</table>

To protect these users from unauthorized use:
- Define a new superuser and deactivate SAP\*.
- Change all of the default passwords for these users.
- Assign them to the group SUPER so that they only be modified by administrators who are authorized to change users in the group SUPER.
- Lock DDC and EARLYWATCH and unlock them only when necessary.

CLEAR INTENT AND SOPHISTICATED CAPABILITIES
THREAT ACTORS CHAINING VULNERABILITIES

- CVE-2010-5326
- CVE-2020-6287
- CVE-2016-3976
- CVE-2020-6207

**Application Level Access**
- CVE-2018-2380
- CVE-2016-9563

**Other hosts**
(Lateral Movement)

**OS Level Access**

**Ultimate Goal:** Control of mission-critical data and processes
## LIST OF OBSERVED CVEs AND CWEs

<table>
<thead>
<tr>
<th>CVE/CWE</th>
<th>Risk Rating</th>
<th>Date of Patch Release</th>
<th>SAP Support Note (patch information)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2016-9563</td>
<td>Medium</td>
<td>Aug 08, 2016</td>
<td><a href="https://launchpad.support.sap.com/#/notes/2296909">https://launchpad.support.sap.com/#/notes/2296909</a></td>
</tr>
<tr>
<td>CVE-2016-3976</td>
<td>High</td>
<td>Mar 8, 2016</td>
<td><a href="https://launchpad.support.sap.com/#/notes/2234971">https://launchpad.support.sap.com/#/notes/2234971</a></td>
</tr>
<tr>
<td>CWE-200</td>
<td>Medium</td>
<td>Mar 07, 2016</td>
<td><a href="https://launchpad.support.sap.com/#/notes/2258786">https://launchpad.support.sap.com/#/notes/2258786</a></td>
</tr>
</tbody>
</table>
**AVERAGE BEHAVIOR AND TIMELINE**

### CONTINUOUS

- **Asset identification scans** continuously look for open ports and SAP applications

### STARTS <72hs after patch release

- **Automated scanning**
  - Reconnaissance

### AUTOMATED EXPLOITATION

- **Exploit creates privileged administrative SAP user in the system.**

### HANDS ON KEYS (MANUAL LOGIN)

- **Attacker logs in manually exploring data and configurations, changing configurations, applying patches etc.**

### PRIVILEGE ESCALATION

- Evasion
- Collection

### QUEST FOR THREAT INTELLIGENCE

Enhanced ability to observe the full lifecycle of attacks

### STARTS few hours post-exploit

- **Financial fraud in SAP apps**
- **Data exfiltration of SAP info**
- **Disruption of SAP-based processes**

Onapsis Inc. | All Rights Reserved
Threat actors are actively targeting and exploiting unsecured SAP applications. They possess the expertise and capabilities to carry out sophisticated attacks.

The window to defend is short: Exploitation starts <72hrs after the SAP patch is released. New SAP systems provisioned in cloud (IaaS) environments being discovered and attacked about 3 hours.

Attacks target not only missing SAP security patches as vectors, but also unsecured configurations. The exploited gaps are present in the majority of SAP implementations assessed by Onapsis.

These threats not only represent a significant cybersecurity risk, they also have material regulatory compliance (SOX, GDPR, etc.) implications.
Specific Actionable Intelligence

We strongly recommend performing a *compromise assessment* of mission-critical and at-risk SAP applications, evaluating the following indicators and context:

1. Any SAP applications configured with high-privileged users with weak and/or default passwords.
2. Any SAP applications that were vulnerable to CVE-2020-6287 and were unpatched as of *July 23rd, 2020*.
3. Any SAP applications vulnerable to CVE-2020-6207 and unpatched as of *October 19th, 2020*.
4. Any SAP applications vulnerable to CVE-2010-5326 at any given period of time, but especially as of *May 11th, 2016*.
5. Any SAP applications vulnerable to CVE-2018-2380, CVE-2016-9563, or CVE-2016-3976.

When immediate patching is not possible, deploy real time threat monitoring as a *compensating control*. 
SAP & Onapsis Recommend Immediate Action

Given the level of observed threat actor’s capabilities and widespread nature of the ongoing threat activity, SAP and Onapsis are proactively alerting organizations to take immediate action including:

- Performing a **compromise assessment** and forensic investigation of at-risk environments
- **Swift application** of the relevant SAP security patches
- Thorough review of **security configuration** of their SAP landscapes
- When immediate patching is not possible, deploying **real time threat monitoring as a compensating control**.
BUSINESS AND REGULATORY COMPLIANCE IMPACT

SUCCESSFUL EXPLOITATION WOULD ALLOW ATTACKERS TO:

- Steal PII from employees, customers and suppliers
- Read, modify or delete financial records
- Change banking details (account numbers, IBAN numbers, etc)
- Administer purchasing processes
- Disrupt critical business operations
- Perform unrestricted actions through OS command execution
- Delete or modify traces, logs and other files

UNPROTECTED SYSTEMS COULD CAUSE COMPLIANCE DEFICIENCIES:

- Data privacy (GDPR, CCPA, others) due to unauthorized access of protected data regardless of exfiltration
- Financial reporting (SOX) due to unauthorized changes to financial data or bypassing of internal controls causing inaccurate financial reporting
- Industry-specific regulations (NERC CIP, PCI-DSS, others) due to impact on regulated data
THANK YOU

@onapsis

linkedin.com/company/onapsis/

WWW.ONAPSIS.COM
# APPENDIX A

## LIST OF CVES AND CWES OF CONCERN

<table>
<thead>
<tr>
<th>CVE/CWE</th>
<th>Risk Rating</th>
<th>Date of Patch Release</th>
<th>SAP Support Note (patch information)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2016-9563</td>
<td>Medium</td>
<td>Aug 08, 2016</td>
<td><a href="https://launchpad.support.sap.com/#/notes/2296909">https://launchpad.support.sap.com/#/notes/2296909</a></td>
</tr>
<tr>
<td>CVE-2016-3976</td>
<td>High</td>
<td>Mar 8, 2016</td>
<td><a href="https://launchpad.support.sap.com/#/notes/2234971">https://launchpad.support.sap.com/#/notes/2234971</a></td>
</tr>
<tr>
<td>CWE-200</td>
<td>Medium</td>
<td>Mar 07, 2016</td>
<td><a href="https://launchpad.support.sap.com/#/notes/2258786">https://launchpad.support.sap.com/#/notes/2258786</a></td>
</tr>
</tbody>
</table>
Onapsis has observed the following URLs being target of HTTP requests as part of exploitation or exploitation attempts to compromise or expand the compromise within SAP applications:

- [POST] /CTCWebService/CTCWebServiceBean
- [POST] /EemAdminService/EemAdmin
- [GET] /ctc/servlet/com.sap.ctc.util.ConfigServlet
- [GET] /sap/admin/public
- [GET] /sap/admin/publicicp
- [POST] /b2b/admin/logging.jsp
- [GET] /b2b/init.do?%22[MALICIOUS_INPUT]%22
- [POST] /b2b/admin/logging.jsp
- [POST] /sap.com~tc~bpem~him~uwlcnn~provider~web/bpemuwlcnn
- [GET] /CrashFileDownloadServlet?fileName=<PATH_TO_FILE>

Administrators should search the SAP Application Server logs for the evidence of execution of the previously listed requests. The logs can be found at the following paths:

- (Unix/Linux) /usr/sap/<SID>/<INSTANCE>/j2ee/cluster/server<NODE>/log
- (Windows) DRIVE:/usr/sap/<SID>/<INSTANCE>/j2ee/cluster/server<NODE>/log

The following non-standard user agents were observed in connection with exploitation and post exploitation:

- Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 CVE-2020-6287 PoC
- Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 CVE-2020-6286 PoC
- Nuclei - Open-source project (github.com/projectdiscovery/nuclei)
- python-requests/2.25.0
- python-requests/2.24.0
- python-requests/2.23.0
Onapsis has seen attackers connect to compromised SAP applications from certain IP addresses. Although these IPs might be temporary, responders should investigate these IP addresses on their networks and act accordingly.

<table>
<thead>
<tr>
<th>Source IP Addresses</th>
<th>Source IP Addresses</th>
<th>Source IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>103.219.193[.]177</td>
<td>156.146.43[.]201</td>
<td>213.232.87[.]201</td>
</tr>
<tr>
<td>103.219.193[.]212</td>
<td>157.7.132[.]28</td>
<td>218.187.66[.]134</td>
</tr>
<tr>
<td>108.160.136[.]124</td>
<td>158.247.199[.]115</td>
<td>69.4.234[.]30</td>
</tr>
<tr>
<td>123.16.77[.]127</td>
<td>167.172.200[.]181</td>
<td>86.106.103[.]116</td>
</tr>
<tr>
<td>124.248.219[.]232</td>
<td>172.104.121[.]252</td>
<td>95.30.32[.]65</td>
</tr>
<tr>
<td>128.199.69[.]229</td>
<td>181.143.12[.]194</td>
<td></td>
</tr>
<tr>
<td>134.35.60[.]210</td>
<td>185.120.124[.]27</td>
<td></td>
</tr>
<tr>
<td>139.162.12[.]191</td>
<td>190.2.131[.]159</td>
<td></td>
</tr>
<tr>
<td>139.162.48[.]186</td>
<td>199.195.251[.]198</td>
<td></td>
</tr>
<tr>
<td>153.122.160[.]135</td>
<td>210.121.187[.]8</td>
<td></td>
</tr>
</tbody>
</table>