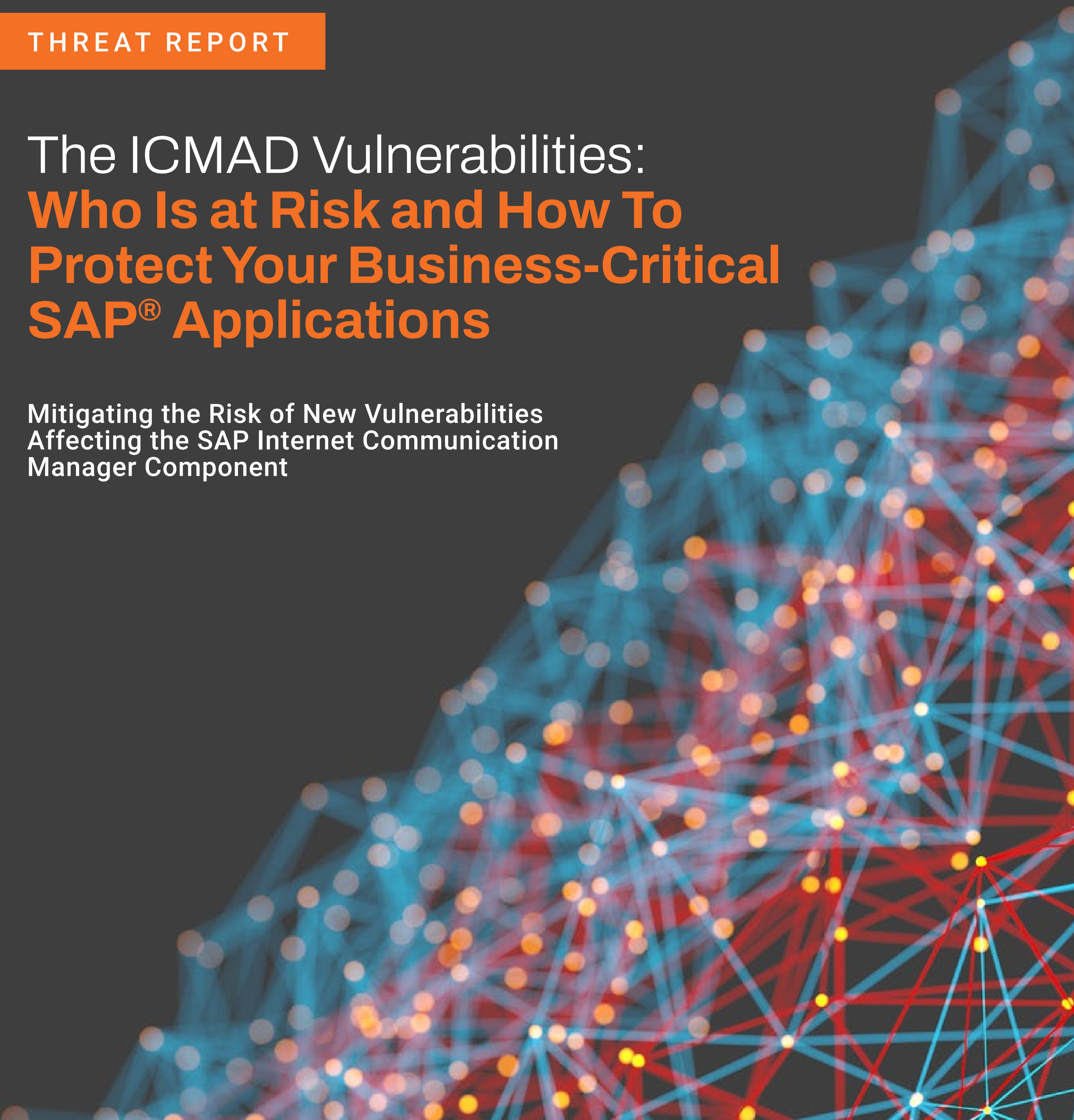
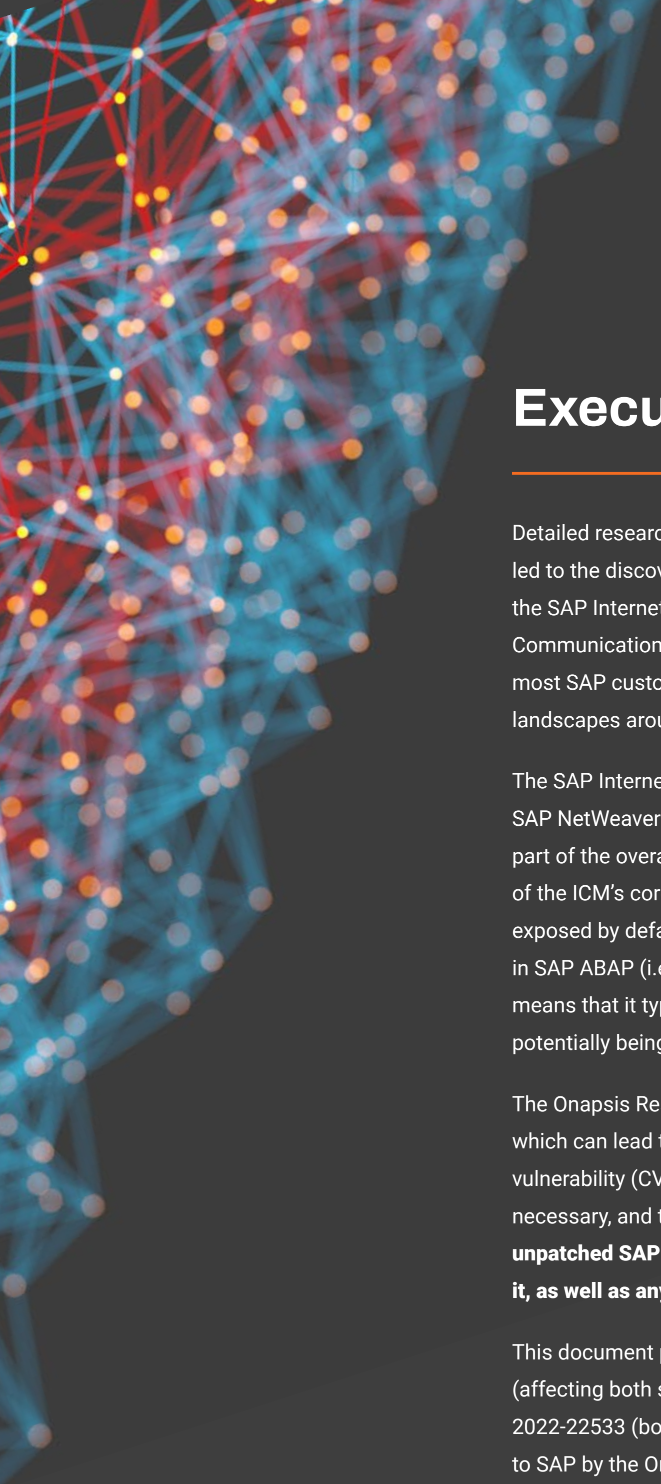
THREAT REPORT

# The ICMAD Vulnerabilities: Who Is at Risk and How To Protect Your Business-Critical SAP® Applications

## Mitigating the Risk of New Vulnerabilities Affecting the SAP Internet Communication Manager Component



# Table of Contents



# Executive Summary

Detailed research from the Onapsis Research Labs over the past year in HTTP Response Smuggling led to the discovery of a set of critical vulnerabilities affecting SAP applications actively using the SAP Internet Communication Manager (ICM), which we are referring to as ICMAD (Internet Communication Manager Advanced Desync). This discovery requires immediate attention by most SAP customers, given the widespread usage of the vulnerable technology component in SAP landscapes around the world.

The SAP Internet Communication Manager (ICM) is one of the most important components of an SAP NetWeaver application server. This component is present in most SAP products and is a critical part of the overall SAP technology stack, connecting SAP applications with the Internet. Because one of the ICM's core purposes is to serve as the SAP HTTP(S) server, this service is always present and exposed by default in SAP NetWeaver Java applications and is a requirement to run web applications in SAP ABAP (i.e., Web Dynpro). Additionally, the SAP ICM is part of the SAP Web Dispatcher, which means that it typically sits between most SAP application servers and the clients (with the clients potentially being the Internet).

The Onapsis Research Labs identified three critical vulnerabilities in a memory handling mechanism which can lead to full system takeover, if exploited by an attacker. Leveraging the most critical vulnerability (CVSSv3 10.0) is simple, requires no previous authentication, no preconditions are necessary, and the payload can be sent through HTTP(S). **Therefore, with this most critical issue, unpatched SAP NetWeaver applications (JAVA/ABAP) reachable through HTTP(S) are vulnerable to it, as well as any application sitting behind SAP Web Dispatcher, such as S/4HANA.**

This document provides an overview of this set of critical vulnerabilities, namely CVE-2022-22536 (affecting both stacks and applications behind the SAP Web Dispatcher), CVE-2022-22532, and CVE-2022-22533 (both of which affect SAP AS Java systems only), that were discovered and reported to SAP by the Onapsis Research Labs. CVE-2022-22536, scored with CVSSv3 of 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H), can be exploited by malicious threat actors to compromise any SAP NetWeaver Java or ABAP application with default configurations. This can be achieved using a single request through the commonly exposed HTTP(S) service, without any authentication required.

The Onapsis Research Labs were able to validate that attackers could use these issues in the ICM to exploit and hijack a victim SAP user's requests (including their sessions) and subsequently take over the SAP application. In addition, using the new HTTP Response Smuggling techniques **presented by Onapsis in 2021**, attackers could control responses sent by the SAP application and persist the attack. This means that with a single request, an attacker would be able to steal every victim session and credentials in plain text and modify the behavior of the applications. The business impact here can potentially range from simply hijacking user identities or stealing user's confidential information to a complete takeover of a critical SAP application, leading to security events that could disrupt business operations or potentially expose an organization to greater risk.

What makes these vulnerabilities particularly critical for SAP customers is the fact that the issues are present by default in the ICM component. A simple HTTP request, indistinguishable from any other valid message and without any kind of authentication, is enough for a successful exploitation. Consequently, this makes it easy for attackers to exploit it and more challenging for security technology such as firewalls or IDS/IPS to detect it (as it does not present a malicious payload).

Onapsis worked in close partnership with SAP to report the vulnerabilities and provide the technical details and support to help fix these critical vulnerabilities. Onapsis would like to thank the SAP Product Security Response Team (PSRT) for their collaboration and timely response. The two teams worked tirelessly to ensure that a timely fix was available to all SAP customers, as soon as possible.

To address these vulnerabilities, SAP has released SAP HotNews Security Notes 3123396 and 3123427. The U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) has listed these vulnerabilities on its **Current Activity Alerts webpage**. CISA, SAP, and Onapsis strongly advise that all impacted organizations should apply these security notes as soon as possible, prioritizing those affected systems exposed to untrusted networks, such as the Internet.

# Background

The SAP Internet Communication Manager (ICM) is one of the most important components of an SAP NetWeaver Application server, as it allows for the communication of the SAP system with the outside world (i.e., the Internet). Even though the ICM can understand and handle different protocols such as P4, IIOP, SMTP, and others, one of its core purposes is to work as the SAP HTTP(S) server. This service is always present and exposed by default in an SAP Java stack and is required to run web applications in SAP ABAP (Web Dynpro) and S/4HANA systems. Additionally, the SAP ICM is part of the SAP Web Dispatcher, which means that it typically sits between most SAP application servers and the clients (with the clients potentially being the Internet).

To process HTTP(S) requests, the ICM first receives the client's payload, parses it to determine how the message should be handled, and, in most cases, forwards the input data to the corresponding Java/ABAP application. To do so, it places the message on a buffer in the shared memory of the operating system (OS) using a group of data structures and functions called Memory Pipes (MPI). MPI Buffers are special from other memory areas because different processes in the OS, such as the ICM and the Java/ABAP work processes, share the same region. Therefore, it can be used to transfer data between them.

The Onapsis Research Labs identified three critical vulnerabilities in a memory handling mechanism which can lead to full system takeover, if exploited by an attacker. Leveraging the most critical vulnerability (CVSSv3 10.0) is simple, requires no previous authentication, no preconditions are necessary, and the payload can be sent through HTTP(S), the most widely used network service to access SAP applications. Therefore, unpatched SAP NetWeaver Applications (JAVA/ABAP), reachable through HTTP(S) are vulnerable to this issue, as well as any application sitting behind SAP Web Dispatcher, such as S/4HANA.

# CVE-2022-22536: MPI Desynchronization

With the highest possible CVSS score (10), the most critical vulnerability is a desynchronization of MPI Buffers between the ICM and the backend (Java/ABAP) processes.

When a request is parsed, the ICM determines which HTTP handlers are required to process it and creates a call hierarchy with a predefined order. The last possible handler is the Java/ABAP invoker that receives the HTTP message through the MPI Buffers. However, this will only happen if no previous handler was able to generate a response for the request. When that's the case, all the next handlers are discarded, and the response is sent back to the client.

For efficiency's sake, all MPI Buffers have the same size. As this size is quite small, one HTTP message may need multiple buffers to be stored. However, since all internal handlers (apart from the Java/ABAP ones) only require the headers of the HTTP request, the ICM only uses and processes the first buffer. The rest of them are placed in the shared memory only when the Java/ABAP handler is called.

The vulnerability described in this section appears when an internal handler is able to generate a response, and the size of the request is bigger than that of the MPI Buffer. If a proxy is placed between the ICM and the clients, an attacker could leverage this to take over the application by exploiting the HTTP desynchronization between both components.

Past research from the Onapsis Research Labs uncovered novel ways that an attacker could exploit previous vulnerabilities, such as CVE-2021-3816. These attacks required multiple interactions between the attacker and the vulnerable component. However, the situation with this vulnerability is different because an attacker only needs a single request to exploit, which makes this attack much simpler. The reason for this is that the desynchronization exists not in the parser but, rather, in the memory manager. Consequently, what this means is that every SAP application sitting behind any kind of proxy with standard configuration will be vulnerable to this issue.

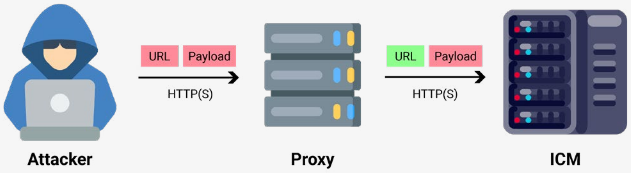
## HTTP Response Smuggling

To exploit the vulnerability, an attacker can use the HTTP Response Smuggling techniques first discovered and **presented by Onapsis Research Labs in 2021**. This allows a client to send a request which will be forwarded by the proxy as one request but split into two at the ICM. For that reason, it is possible to desynchronize the communication between the proxy and the ICM and thereby use HTTP smuggling to hijack a victim's sessions.

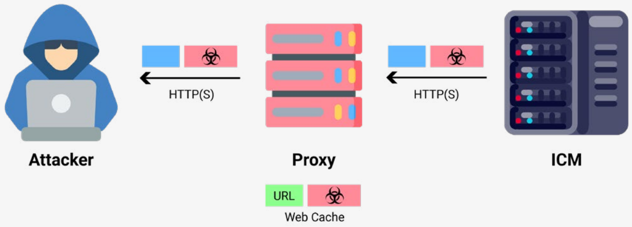
By injecting a malicious payload into the ICM queue, it is possible to control the prefix of the victim's requests (i.e., HTTP Request Smuggling). This can be leveraged by an attacker to hijack user sessions and credentials and completely take over the SAP application.

What's more important, through the use of HTTP Response Smuggling techniques and the characteristics of the aforementioned vulnerability, it is also possible for attackers to poison the proxy's Web Cache and the ICM response queue. This can be accomplished successfully using a single request. In this case, the attack could persist, and all SAP users would be compromised. With one indistinguishable HTTP request, a malicious user can obtain the credentials and client session of arbitrary victim users.

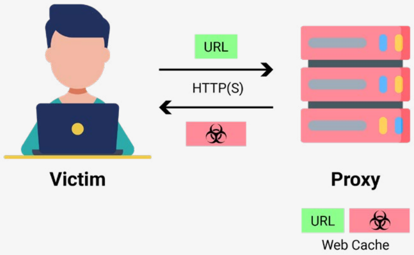
To poison the Web Cache of a proxy, an attacker would send two pipelined (concatenated) requests — the first one containing the malicious payload that will be stored in the cache and the second one with the URL to be poisoned.



This will cause the ICM to return two responses from the malicious payload — the first one with a 2xx/3xx status code and the second with a malicious JavaScript that will be stored as the response of the targeted URL.



Finally, when a victim requests the system for the same URL, which was chosen arbitrarily by the attacker, the malicious response will be returned by the proxy. An attacker could replace every SAP web page with malicious JavaScript.



The Onapsis Research Labs were able to validate that attackers can reliably exploit this issue, which proves that an unauthenticated user can compromise the system if any proxy is present between the ICM and the clients. When HTTP pooling and Web Cache features are disabled in the proxy, it creates a special condition that could reduce the impact of this attack. However, in that case, the next vulnerability can be abused by attackers to achieve the same results but with a different technique.

# CVE-2022-22532: Use After Free in ICM

The second vulnerability reported by Onapsis Research Labs to SAP affects SAP NetWeaver Java systems and is a Use After Free[1] vulnerability in the MPI Buffer management, which holds a CVSS score of 8.1. This score, while not a 10, shouldn't mislead the reader into thinking that it is not a critical vulnerability. Why is this? The three metrics that measure impact (i.e., Confidentiality, Integrity, and Availability) are set to High, and the attack does not require user interaction or authentication. The reason for the slightly lower score is due to the Attack Complexity metric, as they considered some more complex scenarios that could lead to Remote Command Execution. Regardless, as prior Onapsis Research Labs research has demonstrated, threat actors have the knowledge, the technology, and the sophistication to launch complex attacks directly against **business-critical applications such as SAP**.

When multiple requests are sent together, concatenated to the backend using an HTTP feature known as pipelining, the ICM must be capable of splitting them and processing each individually. To do so, it parses the request and finds the end position of the first request. Then, it looks for more bytes after this point. If there are more bytes, the ICM will request a new MPI Buffer and store all the following data as a new request. This buffer will be handled later, once the first request is completed.

Once a response is sent back to a client, the ICM will return the MPI Buffers used, so that other clients' connections can use them. However, when MPI Buffers are freed, there is a call to a function that marks all buffers associated with the connection as unused. This includes the one that will be processed as another isolated request (i.e., via pipelining).

When the second request is processed, the ICM will still have access to the data, as the free function only marks the buffer as unused and does not erase the information. However, in this case, the buffer could also be requested in another connection and affected by another client's request/response.

[1] *Using freed memory | OWASP Foundation*

## Smuggling Without a Proxy

To exploit this issue, an attacker can send a pipelined request with an incomplete message. The ICM will still get a new MPI Buffer but will stop from parsing the second request. This allows the attacker to write more data that will be placed at the beginning of the new buffer. Thus, a malicious threat actor would be able to take control over the SAP application. However, in this case, it is also possible to write arbitrary responses which could be stored in the internal ICM Web Cache. This means that SAP NetWeaver Java is vulnerable to Arbitrary Web Cache poisoning, which can modify the entire behavior of the application. For this reason, all three impact metrics (i.e., Confidentiality, Integrity, Availability) are set to High in the CVSS vectors.

This attack scenario also does not require any proxy to perform smuggling techniques, which makes this vulnerability an interesting and rare case.

## Potential Remote Code Execution

Since MPI Buffers store not only HTTP messages but also control messages (including low-level data structures), it would be possible for attackers to overwrite critical data such as memory buffer lengths or even function pointers. If this happens, an attacker could craft a payload to control internal registers and modify the behavior of the process in order to remotely execute arbitrary code and commands at the OS level with the context of the user that is running all SAP processes.

Additionally, if an attacker is able to obtain privileged credentials (e.g., administrator-level access), it would be possible for them to launch powerful post-exploitation attacks, such as uploading malicious code that would allow them to achieve remote code execution in the affected systems.

# CVE-2022-22533: Memory Leak in MPI Management

The last vulnerability reported by the Onapsis Research Labs is a Memory Leak issue[2] which can lead the ICM to consume all available shared memory resources and cause a denial of service. It has a CVSS score of 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). Research shows that this vulnerability only affects SAP NetWeaver Java systems.

Using this vulnerability, an attacker can easily consume all MPI resources and cause a denial of service attack in any SAP application exposed through the HTTP(S) port, effectively disrupting business processes and interfaces supported by the application.

[2] *Memory leak | OWASP Foundation*

# The Potential Business Impact

A number of facts make these vulnerabilities especially critical:

1. **Detection:** It's challenging to differentiate a malicious request from a perfectly normal, benign request;
2. **Impact:** Many of these vulnerabilities can lead to a full system takeover;
3. **Exploitation:** They require no previous authentication, the exploitation is very simple, and no preconditions are necessary; and
4. **Attack Surface:** The payloads can be sent through HTTP, SAP's most widely used network service, affecting a number of core components that are intended to connect SAP systems to the "outside world."

If an unauthenticated attacker is able to connect to the HTTP(S) service and perform a successful exploitation of these vulnerabilities, the impact to the business could be critical in many scenarios. Technically speaking, an attacker would be able to obtain arbitrary data sent by any user working with the system via HTTP(S) protocol. This means that the attacker could obtain confidential information, usernames and passwords, and session cookies, as well as many other types of data. Further, if an attacker is able to obtain a valid session or a username and password combination, it is entirely possible to impersonate valid users and gain unrestricted access to the system, without the affected user even realizing the ongoing attack.

Due to the wide range of affected SAP applications, it's easy to project a number of impact scenarios that could challenge, disrupt, or expose an organization based on the intention of any attacking threat actor group. Specific impact, of course, varies depending on the affected system, but exploitation of the vulnerabilities allows an attacker to perform several malicious actions:

- Hijack of user identities, theft of all user credentials and personal information
- Exfiltration of sensitive or confidential corporate information
- Fraudulent transactions and financial harm
- Change of banking details in a financial system of record
- Internal denial of service attack that disrupts critical systems for the business

Furthermore, for many organizations, SAP applications fall under the purview of specific industry and governmental regulations, financial, and other compliance requirements. The presence of known vulnerabilities in SAP applications that could allow unauthenticated, unfettered access would constitute a deficiency in IT controls for data privacy (e.g., GDPR, CCPA), financial reporting (e.g., SOX), and industry-specific regulations (e.g., NERC CIP, PCI DSS). Any enforced controls that are bypassed via exploitation of these vulnerabilities may cause regulatory and compliance deficiencies over critical areas. If in doubt, please connect with internal risk, compliance, and legal teams regarding specific regulatory and other compliance requirements applicable to the organization.

# Protecting Your SAP Business Applications

Onapsis worked in close partnership with the SAP Product Security Response Team (PSRT) to address these issues, providing technical details, proof-of-concept code, and more to be analyzed by the SAP Security team. As a result of this collaboration and the tireless work of the SAP PSRT, SAP was able to release HotNews Security Notes 3123396 and 3123427 as part of the regular monthly Security Patch Day in February 2022.

Onapsis Research Labs recommends analyzing the impact that the issues described above can have on your landscape (specifically considering if you have SAP systems exposed to the Internet or to untrusted networks) and applying the notes as soon as possible. For additional guidance about available workarounds for these vulnerabilities, SAP customers should check the References and Workarounds section in the corresponding SAP Security Notes.

## Onapsis Platform Support

The Onapsis Platform includes vulnerability assessment capabilities, detection rules, and alarms to continuously monitor malicious activity targeting these specific vulnerabilities as well as many others. With the first release of February 2022 (2.2022.021), all Onapsis customers with **Onapsis Assess** and/or **Onapsis Defend** have the capabilities to protect their organizations against these critical issues.

## Free ICMAD Vulnerability Scanning Tool

Given the criticality of these vulnerabilities, especially in light of our increasingly interconnected world, Onapsis would like to ensure that every SAP customer can check to see if they are exposed — and take steps to protect their business-critical SAP applications. As part of our responsible outreach to the global SAP community, the Onapsis Research Labs have created a free vulnerability scanning tool that will allow any SAP customer to scan for applications across their SAP landscape that are affected by these vulnerabilities.

**You can download this free tool here.**

# Conclusion

The aforementioned vulnerabilities present a critical risk to all unprotected SAP applications that are not patched with the corresponding SAP Security Notes.[3] Without taking prompt action to mitigate this risk, it's possible that an unauthenticated attacker could fully compromise any unpatched SAP system in a simple way.

Today's threat actors already have the knowledge and capabilities to compromise unprotected business applications. Threat intelligence **from SAP, CISA, and Onapsis** has demonstrated that threat actors are launching sophisticated attacks on business-critical SAP applications within 72 hours of the release of an SAP Security Note. In December 2021, Onapsis Research Labs saw attacks within **24 hours of the public disclosure of the Log4j exploit**.

These notes are rated with the highest CVSS scores and affect commonly deployed components in multiple, widely deployed products from SAP. It is also important to highlight that the affected components, by design, are intended to be exposed to the Internet, thereby greatly increasing the risk that any attacker, with access to the HTTP(S) port of a Java or ABAP system, could take over the applications and, in some circumstances, even the host OS.

Furthermore, because in scenarios involving SAP NetWeaver Java systems, exploitation does not necessarily require a proxy between the ICM and the client, SAP and Onapsis believe that all unpatched SAP applications are at risk and strongly advise all impacted organizations to prioritize patching these affected systems as soon as possible.

[3] *SAP Security Notes - SAP Support Launchpad*

## Request a Cybersecurity Briefing

For SAP customers not currently using The Onapsis Platform, set up a complimentary security briefing with Onapsis experts to help identify these vulnerabilities (and others) in your SAP systems.

**REQUEST A BRIEFING HERE**

## About The 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 business-critical applications, such as SAP, Oracle, 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 keep customers running The Onapsis Platform steps ahead of ever-evolving cybersecurity threats.

ONAPSIS

### ABOUT ONAPSIS

Onapsis protects the cloud, hybrid, and on-premises business-critical applications that run the global economy, including ERP, CRM, PLM, HCM, SCM, and BI applications from SAP, Oracle, Salesforce, and other SaaS platforms. Onapsis proudly protects more than 300 global brands and partners with leading consulting and audit firms such as Accenture, Deloitte, IBM, PwC, and Verizon. Learn more at https://www.onapsis.com.