# Onapsis Security Advisory 2022-0001: HTTP Request Smuggling in SAP Web Dispatcher

From: Onapsis Research via Fulldisclosure <fulldisclosure () seclists org>
Date: Wed, 4 May 2022 13:17:29 -0300

# Onapsis Security Advisory 2022-0001: HTTP Request Smuggling in SAP Web Dispatcher

## Impact on Business

By injecting an HTTP request as a prefix into a victim's request, a malicious user is able to cause damage in different ways, such as producing a Denial of Service by setting an invalid request as a prefix.

It is also possible to inject a valid prefixed request that will include the victim's information from its original request. This can be leveraged to perform malicious requests with the victim's credentials or information, or even steal user data.

HTTP smuggling can also be combined with other vulnerabilities such as a XSS or reflected content (not vulnerability by itself), by injecting a request to the vulnerable application/web page as a prefix. If the attacker is able to set the prefix of the victim request and also knows a reflected XSS (it can also work with other content reflection), then the response will include a malicious script that will be executed on the victim's browser.

This vulnerability is also useful to perform Web Cache Poisoning.
The HTTP caches in the different layers will see valid requests for which the response should be stored (considered static), but the actual request is modified by the prefix of the attacker to retrieve another resource, which should not be stored in the cache.
As an example, if a user requests an image, the server will probably cache the response as the resource is static. However, if this request is prefixed by another request which returns sensible data, such as personal information, then this response will be stored in the cache. Therefore, when the attacker requests the same image, all the victim's personal information will be retrieved.

Finally, a critical information disclosure could end up in session hijacking and further attacks. This can be performed by combining HTTP Desynchronization with Open Redirect, and use the victim's request as the parameter of the redirect location. This would force the victim to send its original request to the attacker, including critical data such as session cookies or query parameters.

## Advisory Information

- Public Release Date: 04/05/2022
- Security Advisory ID: ONAPSIS-2022-0001
- Researcher(s): Martin Doyhenard, Yvan Genuer

## Vulnerability Information

- Vendor: SAP
- Affected Components:
  - KRNL64NUC 7.22, 7.22EXT, 7.49
  - KRNL64UC 7.22, 7.22EXT, 7.49, 7.53
  - WEBDISP 7.53, 7.77, 7.81
  - KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.83

  (Check SAP Note 3080567 for detailed information on affected releases)

- Vulnerability Class: CWE-444
- CVSS v3 score: 8.9 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:L
- Risk Level: High
- Assigned CVE: CVE-2021-38162
- Vendor patch Information: SAP Security NOTE 3080567

## Affected Components Description

The SAP Web dispatcher works as a frontend server between the Internet and one or more backend systems. Which consists of one or more SAP Netweaver ABAP, SAP Netweaver JAVA, SAP HANA, as well as third party application servers.

## Vulnerability Details

An HTTP desynchronization vulnerability, TE.CL type is present in SAP Web Dispatcher if the parameter ```wdisp/HTTP/use_pool_for_new_conn``` is enabled.

Pool connection related SAP Note :

 * 2007212 - Tuning SAP Web Dispatcher and ICM for high load

 * 953784 - SAP Web Dispatcher Connection Pooling

If an attacker sends both HTTP headers "Content-Length" (CL) and "Transfer-Encoding" (TE) in the same HTTP request, the SAP Webdispatcher processes the TE header and treats the message body as using chunked encoding.
This request is forwarded on to the SAP system ICM service, which processes only the CL header and determines the body size with it. The rest of the request are

left unprocessed and the ICM will treat it as being the start of the next
request
in the sequence.

This can be leveraged to gain control of requests issued by other users, and
even obtain sensitive information by retrieving the victim's requests and
responses.

## Solution

SAP has released SAP Note 3080567 which provides patched versions of the
affected components.

The patches can be downloaded from
https://launchpad.support.sap.com/#/notes/3080567.

Onapsis strongly recommends SAP customers to download the related
security fixes and apply them to the affected components in order to
reduce business risks.

## Report Timeline

- 07/12/2021: Onapsis sends details to SAP
- 07/12/2021: SAP provides internal ID
- 08/09/2021: Vulnerability in progress
- 09/14/2021: SAP releases SAP Note fixing the issue.
- 05/04/2022: Advisory Published

## References

- Onapsis blogpost:
https://www.onapsis.com/blog/sap-security-patch-day-september-2021
- CVE Mitre:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38162
- Vendor Patch:
https://launchpad.support.sap.com/#/notes/3080567

## About Onapsis Research Labs

Onapsis Research Labs provides the industry analysis of key security
issues that impact business-critical systems and applications.
Delivering frequent and timely security and compliance advisories with
associated risk levels, Onapsis Research Labs combine in-depth knowledge
and experience to deliver technical and business-context with sound
security judgment to the broader information security community.

Find all reported vulnerabilities at
https://github.com/Onapsis/vulnerability_advisories

## About Onapsis, Inc.

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, while keeping them protected and compliant.

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

--

⬅ By Date ➡ ⬅ By Thread ➡

Current thread:

Onapsis Security Advisory 2022-0001: HTTP Request Smuggling in SAP Web Dispatcher ***Onapsis Research via Fulldisclosure (May 04)***

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License