SAP Web Dispatcher HTTP Request Smuggling

Authored by Yvan Genuer, Martin Doyhenard | Site onapsis.com

Posted May 4, 2022

SAP Web Dispatcher suffers from an HTTP request smuggling vulnerability.

tags | exploit, web
advisories | CVE-2021-38162
SHA-256 | 13d3e2b23a840dab61234f2b6d3787259a7efde984a35e90339e0cdc4c879d9a

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# 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
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
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.

--
This email and any files transmitted with it are confidential and intended
solely for the use of the individual or entity to whom they are addressed.
If you have received this email in error please notify the system manager.
This message contains confidential information and is intended only for the
individual named. If you are not the named addressee you should not
disseminate, distribute or copy this e-mail.
Please notify the sender
immediately by e-mail if you have received this e-mail by mistake and
delete this e-mail from your system. If you are not the intended recipient
you are notified that disclosing, copying, distributing or taking any
action in reliance on the contents of this information is strictly
prohibited.
```

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Login or Register to add favorites

packet storm
© 2022 Packet Storm. All rights reserved.

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter
Subscribe to an RSS Feed