



Site Search



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)

List Archive Search



Onapsis Security Advisory 2021-0007: Exposure of Sensitive Information to an Unauthorized Actor

From: Onapsis Research via Fulldisclosure <fulldisclosure () seclists.org>
Date: Mon, 14 Jun 2021 13:31:08 -0300

Onapsis Security Advisory 2021-0007: Exposure of Sensitive Information to an Unauthorized Actor

Impact on Business

An attacker can generate download-links sequentially targeting "impex" directory files. As a consequence, they will be able download most of these files, potentially disclosing critical Hybris information such as credentials.

Advisory Information

- Public Release Date: 06/14/2021
- Security Advisory ID: ONAPSIS-2021-0007
- Researcher: Gaston Traberg

Vulnerability Information

- Vendor: SAP
- Affected Components:
 - SAP Hybris eCommerce 1808
 - SAP Hybris eCommerce 1811
 - SAP Hybris eCommerce 1905
 - SAP Hybris eCommerce 2005
- Vulnerability Class: [CWE-200] Exposure of Sensitive Information to an Unauthorized Actor
- CVSS v3 score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
- Risk Level: High
- Assigned CVE: CVE-2020-26809
- Vendor patch Information: SAP Security NOTE 2975189

Affected Components Description

SAP Hybris is an ecommerce platform that is used to address a family of products involving Customer Experience and Management. The "medias" module is responsible for providing users a secure way to upload and access files in the system.

Vulnerability Details

When a file is uploaded into Hybris using the "medias" module, part of the destination path is generated using user-provided information and some other static context data kept by Hybris. The user-controlled part is the only one that changes among uploaded files and therefore it's possible to sequentially craft download-links (bruteforcing) with the goal of accessing prior uploaded files. Among these files it is possible to find critical ones such as those inside the 'impex' directory.

Solution

SAP has released SAP Note 2975189 which provide patched versions of the affected components.

The patches can be downloaded from <https://service.sap.com/sap/support/notes/2975189>.

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

- 08-25-2020: Onapsis provides details to SAP
- 08-25-2020: SAP provides SR ID
- 09-09-2020: SAP provides update: "Vulnerability is in progress"
- 10-12-2020: SAP provides update: "Fix in progress"
- 02-09-2021: SAP releases SAP Note fixing the issue. Vulnerability is now closed

References

- * Onapsis blogpost: <https://onapsis.com/blog/sap-security-notes-november-2020>
- * CVE Mitre: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26809>
- * Vendor Patch: <https://launchpad.support.sap.com/#/notes/2975189>

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>.

License

This advisory is licensed under a [Creative Commons 4.0 BY-ND International License] (<https://creativecommons.org/licenses/by-nd/4.0/legalcode>)

--

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.





Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <http://seclists.org/fulldisclosure/>

◀ By Date ▶ ▶ By Thread ▶

Current thread:

Onapsis Security Advisory 2021-0007: Exposure of Sensitive Information to an Unauthorized Actor *Onapsis Research* via *Fulldisclosure* (Jun 14)

Site Search

Nmap Security Scanner	Npcap packet capture	Security Lists	Security Tools	About	 
Ref Guide	User's Guide	Nmap Announce	Vuln scanners	About/Contact	
Install Guide	API docs	Nmap Dev	Password audit	Privacy	 
Docs	Download	Full Disclosure	Web scanners	Advertising	
Download	Npcap OEM	Open Source Security	Wireless	Nmap Public Source License	
Nmap OEM		BreachExchange	Exploitation		