Advisory Alert

Alert Number: AAA20230912 **Date:** September 12, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**Medium**	Information Disclosure Vulnerability
OpenSSL	**Low**	Denial of service Vulnerability

Description

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-40622, CVE-2022-41272, CVE-2023-25616, CVE-2023-40309)
Description	SAP has released a security update addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead Information Disclosure, Improper access control, Missing Authorization check. SAP highly recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	SAP Business Client, Versions - 6.5, 7.0, 7.70 SAP BusinessObjects Business Intelligence Platform (Promotion Management), Versions – 420, 430 SAP NetWeaver Process Integration, Version – 7.50 SAP Business Objects Business Intelligence Platform (CMC), Versions – 420, 430 SAP CommonCryptoLib, Versions – 8 SAP NetWeaver AS ABAP, SAP NetWeaver AS Java and ABAP Platform of S/4HANA on-premise, Versions - KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KERNEL 7.22, KERNEL 8.04, KERNEL64UC 7.22, KERNEL64UC 7.22EXT, KERNEL64UC 7.53, KERNEL64UC 8.04, KERNEL64NUC 7.22, KERNEL64NUC 7.22EXT SAP Web Dispatcher, Versions - 7.22EXT, 7.53, 7.54, 7.77, 7.85, 7.89 SAP Content Server, Versions - 6.50, 7.53, 7.54 SAP HANA Database, Versions – 2.0 SAP Host Agent, Versions – 722 SAP Extended Application Services and Runtime (XSA), Versions - SAP_EXTENDED_APP_SERVICES 1, XS_ADVANCED_RUNTIME 1.00 SAPSSOEXT, Versions – 17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=100

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42472, CVE-2023-40308, CVE-2023-40621, CVE-2023-40623, CVE-2023-40306, CVE-2021-41184, CVE-2021-41183, CVE-2021-41182, CVE-2023-24998, CVE-2023-40624, CVE-2023-40625, CVE-2023-37489, CVE-2023-41367, CVE-2023-41369, CVE-2023-41368)
Description	SAP Hat has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Information Disclosure, Missing Authentication check, Code Injection SAP recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), Versions – 420 SAP CommonCryptoLib, Versions – 8 SAP NetWeaver AS ABAP, SAP NetWeaver AS Java and ABAP Platform of S/4HANA on-premise, Versions - KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KERNEL 7.22, KERNEL 8.04, KERNEL64UC 7.22, KERNEL64UC 7.22EXT, KERNEL64UC 7.53, KERNEL64UC 8.04, KERNEL64NUC 7.22, KERNEL64NUC 7.22EXT SAP Web Dispatcher, Versions - 7.22EXT, 7.53, 7.54, 7.77, 7.85, 7.89 SAP Content Server, Versions - 6.50, 7.53, 7.54 SAP HANA Database, Versions – 2.0 SAP Host Agent, Versions – 722 SAP Extended Application Services and Runtime (XSA), Versions - SAP_EXTENDED_APP_SERVICES 1, XS_ADVANCED_RUNTIME 1.00 SAPSSOEXT, Versions –17 SAP PowerDesigner Client, Version – 16.7 SAP BusinessObjects Suite (Installer), Versions – 420, 430 SAP S/4HANA (Manage Catalog Items and Cross-Catalog search), Versions – S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106 SAPUI5, Versions – SAP_UI 750, SAP_UI 753, SAP_UI 754, SAP_UI 755, SAP_UI 756, UI_700 200 SAP Quotation Management Insurance (FS-QUO), Versions – 400, 510, 700, 800 SAP NetWeaver AS ABAP (applications based on Unified Rendering), Versions – SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, SAP_BASIS 702, SAP_BASIS 731 S4CORE (Manage Purchase Contracts App), Versions – 102, 103, 104, 105, 106, 107 SAP BusinessObjects Business Intelligence Platform (Version Management System), Versions – 430 SAP NetWeaver (Guided Procedures), Version – 7.50 SAP S/4HANA (Create Single Payment application), Versions – 100, 101, 102, 103, 104, 105, 106, 107, 108 S4 HANA ABAP (Manage checkbook apps), Versions – 102, 103, 104, 105, 106, 107
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=100

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2022-40982)
Description	HPE has released a security update addressing an Information Disclosure s that exist in the third-party components that in turn affect HPE Superdome Flex servers. The vulnerability could be locally exploited to allow disclosure of information. HPE recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	HPE Superdome Flex Server - Prior to v3.80.24
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04534en_us

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Denial of service Vulnerability (CVE-2023-4807)
Description	OpenSSL has released a security update addressing Denial of service Vulnerability due to insufficient validation of user-supplied input within the POLY1305 MAC implementation. A remote attacker can send specially crafted input to the application and corrupt MM registers on Windows 64 platform, resulting in a denial of service condition. OpenSSL recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	OpenSSL versions 1.1.1 to 1.1.1v, 3.0.0 to 3.0.10, and 3.1.0 to 3.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20230908.txt

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.