TLP: WHITE

Advisory Alert

Alert Number: **AAA20230613** **Date:** **June 13, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**Critical**	Heap-based buffer overflow Vulnerability
IBM	**High**	Denial of service Vulnerability
Fortinet	**High, Medium, Low**	Multiple Vulnerabilities
SAP	**High, Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Heap-based buffer overflow vulnerability (CVE-2023-27997)
Description	Fortinet has released a security update addressing heap-based buffer overflow vulnerability in their FortiOS and FortiProxy SSL-VPN. Exploitation could result in remote code execution and information disclosure. Fortinet highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	FortiOS-6K7K version 7.0.10 FortiOS-6K7K version 7.0.5 FortiOS-6K7K version 6.4.12 FortiOS-6K7K version 6.4.10 FortiOS-6K7K version 6.4.8 FortiOS-6K7K version 6.4.6 FortiOS-6K7K version 6.4.2 FortiOS-6K7K version 6.2.9 through 6.2.13 FortiOS-6K7K version 6.2.6 through 6.2.7 FortiOS-6K7K version 6.2.4 FortiOS-6K7K version 6.0.12 through 6.0.16 FortiOS-6K7K version 6.0.10 FortiProxy version 7.2.0 through 7.2.3 FortiProxy version 7.0.0 through 7.0.9 FortiProxy version 2.0.0 through 2.0.12 FortiProxy 1.2 all versions FortiProxy 1.1 all versions FortiOS version 7.2.0 through 7.2.4 FortiOS version 7.0.0 through 7.0.11 FortiOS version 6.4.0 through 6.4.12 FortiOS version 6.0.0 through 6.0.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-097

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-28867)
Description	IBM has identified denial of service vulnerability in IBM WebSphere, In GraphQL Java (aka graphql-java) before 20.1, an attacker can send a crafted GraphQL query that causes stack consumption. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM WebSphere Hybrid Edition 5.1 IBM WebSphere Application Server Liberty 17.0.0.3 - 23.0.0.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7003245

Affected Product	**Fortinet**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-26210, CVE-2023-28000, CVE-2022-33877, CVE-2023-25609, CVE-2022-39946, CVE-2023-22633, CVE-2023-29178, CVE-2022-43953, CVE-2023-29175, CVE-2023-22639, CVE-2023-26207, CVE-2023-29181, CVE-2023-29180, CVE-2023-29179, CVE-2022-42474, CVE-2023-33305, CVE-2022-42478, CVE-2023-26204, CVE-2022-43949)
Description	Fortinet has released security patch updates addressing multiple vulnerabilities that exists in their products. The exploitation of these vulnerabilities could cause Improper access control, Execute unauthorized code or commands, Information disclosure, Denial of service, Privilege escalation. Fortinet recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	FortiADC 6.0 all versions FortiADC 6.1 all versions FortiADC version 6.2.0 through 6.2.4 FortiADC version 7.0.0 through 7.0.3 FortiADC version 7.1.0 FortiAnalyzer version 6.4.8 through 6.4.11 FortiAnalyzer version 7.0.0 through 7.0.6 FortiAnalyzer version 7.2.0 through 7.2.1 FortiClientWindows version 6.4.0 through 6.4.8 FortiClientWindows version 7.0.0 through 7.0.6 FortiConverter 6.0 all versions FortiConverter 6.2 all versions FortiConverter version 7.0.0 FortiManager version 6.4.8 through 6.4.11 FortiManager version 7.0.0 through 7.0.6 FortiManager version 7.2.0 through 7.2.1 FortiNAC 8.5 all versions FortiNAC 8.6 all versions FortiNAC 8.7 all versions FortiNAC 8.8 all versions FortiNAC 9.1 all versions FortiNAC version 9.2.0 through 9.2.7 FortiNAC version 9.4.0 through 9.4.2 FortiNAC-F version 7.2.0 FortiOS 6.0 all versions FortiOS 6.2 all versions FortiOS 6.4 all versions FortiOS 7.0 all versions FortiOS 7.2 all versions FortiOS version 7.2.0 through 7.2.4 FortiProxy 1.0 all versions FortiProxy 1.1 all versions FortiProxy 1.2 all versions FortiProxy 2.0 all versions FortiProxy 7.0 all versions FortiProxy version 2.0.0 through 2.0.11 FortiProxy version 7.2.0 through 7.2.1 FortiProxy version 7.2.0 through 7.2.3 FortiSIEM 5.1 all versions FortiSIEM 5.2 all versions FortiSIEM 5.3 all versions FortiSIEM 5.4 all versions FortiSIEM 6.1 all versions FortiSIEM 6.2 all versions FortiSIEM 6.3 all versions FortiSIEM 6.4 all versions FortiSIEM 6.5 all versions FortiSIEM 6.6 all versions FortiSIEM 6.7 all versions FortiSwitchManager version 7.0.0 through 7.0.1 FortiSwitchManager version 7.2.0 through 7.2.1 FortiWeb 6.3 all versions FortiWeb 6.4 all versions FortiWeb version 7.0.0 through 7.0.6 FortiWeb version 7.2.0 through 7.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt?date=06-2023

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-42063, CVE-2023-33991, CVE-2023-2827, CVE-2023-30743, CVE-2022-22542, CVE-2023-33984, CVE-2023-33985, CVE-2023-33986, CVE-2021-42063, CVE-2023-30742, CVE-2023-31406, CVE-2023-32115, CVE-2023-32114)
Description	SAP has released a security update addressing multiple vulnerabilities in their products. If exploited these vulnerabilities could cause Cross-Site Scripting, SQL Injection, Denial of Service, and Information Disclosure. SAP recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SAP Knowledge Warehouse, Versions -7.30, 7.31, 7.40, 7.50 SAP UI5 Variant Management, Versions –SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200 SAP Plant Connectivity, Version –15.5 SAPUI5, Versions –SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200 SAP S/4HANA (Supplier Factsheet and Enterprise Search for Business Partner, Supplier and Customer), Versions -104, 105, 106 SAP NetWeaver (Design Time Repository), Versions -7.50 SAP NetWeaver Enterprise Portal, Versions –7.50 SAP CRM ABAP (Grantor Management), Versions –430 SAP CRM (WebClient UI), Versions–S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 80 SAP BusinessObjects Business Intelligence Platform,Versions–420, 430 Master Data Synchronization (MDS COMPARE TOOL), Version -SAP_APPL 600, 602, 603, 604, 605, 606, 616 SAP NetWeaver (Change and Transport System), Version -702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757
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

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.