Advisory Alert

Alert Number: AAA20240613 **Date:** June 13, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities
FortiGuard	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities
Palo Alto	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29133, CVE-2023-29267, CVE-2023-45853, CVE-2024-25710, CVE-2024-26308, CVE-2024-28757, CVE-2024-28762, CVE-2024-29025, CVE-2024-29131, CVE-2024-31880, CVE-2024-31881)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Db2 . If exploited, these vulnerabilities may lead to Denial of service, Sensitive information disclosure, Arbitrary code execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 10.5.0 - 10.5.11 IBM Db2 11.1.4 - 11.1.4.7 IBM Db2 11.5.0 - 11.5.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7156844 • https://www.ibm.com/support/pages/node/7156845 • https://www.ibm.com/support/pages/node/7156846 • https://www.ibm.com/support/pages/node/7156847 • https://www.ibm.com/support/pages/node/7156848 • https://www.ibm.com/support/pages/node/7156849 • https://www.ibm.com/support/pages/node/7156850 • https://www.ibm.com/support/pages/node/7156851 • https://www.ibm.com/support/pages/node/7156852

Affected Product	**FortiGuard**	
Severity	**High**, **Medium**, **Low**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-23775, CVE-2023-46720, CVE-2024-21754, CVE-2024-23110, CVE-2024-23111, CVE-2024-26010, CVE-2024-31495, CVE-2024-3661)	
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Execute unauthorized code or commands, Improper access control. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.	
Affected Products	FortiClientLinux All versions FortiClientMac All versions FortiClientWindows (IPsec VPN) All versions FortiClientWindows (SSL-VPN) All versions 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 7.4.0 through 7.4.3 FortiOS 7.4.0 through 7.4.1 FortiPAM 1.0 all versions FortiPAM 1.1 all versions FortiPAM 1.2 all versions	FortiPortal 7.0.0 through 7.0.6 FortiPortal 7.2.0 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 7.2 all versions FortiProxy 7.4.0 through 7.4.3 FortiSOAR 7.0 all versions FortiSOAR 7.2.0 FortiSwitchManager 7.0.1 through 7.0.3 FortiSwitchManager 7.2.0 through 7.2.3
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	• https://www.fortiguard.com/psirt/FG-IR-24-128 • https://www.fortiguard.com/psirt/FG-IR-24-036 • https://www.fortiguard.com/psirt/FG-IR-23-471 • https://www.fortiguard.com/psirt/FG-IR-23-495 • https://www.fortiguard.com/psirt/FG-IR-23-460 • https://www.fortiguard.com/psirt/FG-IR-23-423 • https://www.fortiguard.com/psirt/FG-IR-23-356 • https://www.fortiguard.com/psirt/FG-IR-24-170	

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4155, CVE-2023-51779, CVE-2023-52530, CVE-2023-5090, CVE-2023-52639, CVE-2023-52667, CVE-2024-26598)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of service, Use-after-free conditions, code execution. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:3859 • https://access.redhat.com/errata/RHSA-2024:3855 • https://access.redhat.com/errata/RHSA-2024:3854

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20256, CVE-2024-20257, CVE-2024-20258, CVE-2024-20383, CVE-2024-20392)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to HTTP Response Splitting and Cross-Site Scripting. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Secure Email and Web Manager running on Cisco AsyncOS Release 15.0 and earlier Secure Email and Web Manager running on Cisco AsyncOS Release 15.5 Secure Email Gateway running on Cisco AsyncOS Release 14.3 and earlier Secure Email Gateway running on Cisco AsyncOS Release 15.0 Secure Email Gateway running on Cisco AsyncOS Release 15.5 Secure Web Appliance running Cisco AsyncOS Release 14.0 and earlier Secure Web Appliance running Cisco AsyncOS Release 14.5 Secure Web Appliance running Cisco AsyncOS Release 15.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-http-split-GLrnnOwS • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-wsa-xss-bgG5WHOD

Affected Product	**Palo Alto**
Severity	**Medium , Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-5905, CVE-2024-5906, CVE-2024-5907, CVE-2024-5908, CVE-2024-5909)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Cross-site scripting, Privilege escalation, Sensitive information disclosure. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cortex XDR Agent 7.9-CE Versions below 7.9.102-CE on Windows Cortex XDR Agent 8.1 All Cortex XDR Agent 8.2 Versions below 8.2.3 on Windows Cortex XDR Agent 8.3 Versions below 8.3.1 on Windows GlobalProtect App 5.1 Versions below 5.1.12 GlobalProtect App 6.0 Versions below 6.0.8 GlobalProtect App 6.1 Versions below 6.1.3 GlobalProtect App 6.2 Versions below 6.2.3 Prisma Cloud Compute 32 Versions below 32.05 (O'Neal - Update 5)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2024-5905 • https://security.paloaltonetworks.com/CVE-2024-5906 • https://security.paloaltonetworks.com/CVE-2024-5907 • https://security.paloaltonetworks.com/CVE-2024-5908 • https://security.paloaltonetworks.com/CVE-2024-5909

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.