Advisory Alert

Alert Number: **AAA20250128** **Date:** **January 28, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
FortiGuard	**High**	OS Command Injection Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities
phpMyAdmin	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**FortiGuard**
Severity	**High**
Affected Vulnerability	OS Command Injection Vulnerability (CVE-2023-42788)
Description	FortiGuard has released security updates addressing an OS Command Injection Vulnerability that exists in their products. **CVE-2023-42788** - An improper neutralization of special elements used in an OS command vulnerability in FortiManager, FortiAnalyzer & FortiAnalyzer-BigData may allow a local attacker with low privileges to execute unauthorized code via specifically crafted arguments to a CLI command. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiAnalyzer 7.4.0 FortiAnalyzer 7.2 versions 7.2.0 through 7.2.3 FortiAnalyzer 7.0 versions 7.0.0 through 7.0.8 FortiAnalyzer 6.4 versions 6.4.0 through 6.4.12 FortiAnalyzer 6.2 versions 6.2.0 through 6.2.11 FortiAnalyzer-BigData 7.2 versions 7.2.0 through 7.2.5 FortiAnalyzer-BigData 7.0 versions 7.0.1 through 7.0.6 FortiAnalyzer-BigData 6.4 all versions FortiAnalyzer-BigData 6.2 all versions FortiManager 7.4.0 FortiManager 7.2 versions 7.2.0 through 7.2.3 FortiManager 7.0 versions 7.0.0 through 7.0.8 FortiManager 6.4 versions 6.4.0 through 6.4.12 FortiManager 6.2 versions 6.2.0 through 6.2.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-167

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause memory corruption, memory leak, Denial of Service, Use-after-Free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-43904, CVE-2024-40973, CVE-2020-12352, CVE-2024-35967, CVE-2024-50264, CVE-2024-26822, CVE-2020-12351, CVE-2020-24490, CVE-2024-53057, CVE-2024-35965, CVE-2024-38553, CVE-2024-40910, CVE-2024-35966, CVE-2024-35963)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Sensitive Information Disclosure, Arbitrary Code Execution. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7179-4

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-51471, CVE-2024-51470, CVE-2024-52898, CVE-2024-52897, CVE-2024-52896)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM MQ which is shipped with IBM WebSphere Remote Server. These vulnerabilities could be exploited by malicious users to cause Denial of Service and Password Disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Remote Server versions 9.1 and 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7181704

Affected Product	**phpMyAdmin**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-24530, CVE-2025-24529, CVE-2024-2961)
Description	phpMyAdmin has released security updates addressing multiple vulnerabilities that exist in phpMyAdmin administration tool. **CVE-2025-24530** - An XSS vulnerability has been discovered with the phpMyAdmin "Check tables" feature. A specially–crafted table or database name could be used to trigger an XSS attack. **CVE-2025-24529** - An XSS vulnerability has been discovered with the phpMyAdmin "Insert" tab. **CVE-2024-2961** - There was a vulnerability found in glibc/iconv that could potentially affect phpMyAdmin under specific circumstances. phpMyAdmin advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	phpMyAdmin versions 5.x prior to 5.2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.phpmyadmin.net/security/PMASA-2025-1/ • https://www.phpmyadmin.net/security/PMASA-2025-2/ • https://www.phpmyadmin.net/security/PMASA-2025-3/

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.