Advisory Alert

Alert Number: **AAA20240510** **Date:** **May 10, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
F5	**High**	Denial of Service Vulnerability
SonicWall	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
WordPress	**High**	Cross-Site Scripting Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
PostgreSQL	**Low**	Privilege Escalation Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45871)
Description	IBM has issued security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM. Linux Kernel is vulnerable to a buffer overflow, caused by improper bounds checking by the IGB driver in drivers/net/ethernet/intel/igb/igb_main.c. By sending a specially crafted request, a remote attacker could overflow a buffer and execute arbitrary code or cause a denial of service condition on the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP8 IF01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7150684

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-25560)
Description	F5 has released security updates addressing a Denial of Service Vulnerability that exists in Big-IP products. When BIG-IP AFM is licensed and provisioned, undisclosed DNS traffic can cause the Traffic Management Microkernel (TMM) to terminate. Traffic is disrupted while the TMM process restarts. This vulnerability allows a remote unauthenticated attacker to cause a denial-of-service. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next CNF versions 1.1.0 - 1.1.1 BIG-IP (AFM) version 17.1.0 and versions 16.1.0 - 16.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000139037

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29010, CVE-2024-29011)
Description	SonicWall has released security updates addressing multiple vulnerabilities that exist in SonicWall Global Management System. **CVE-2024-29010** - The XML document processed in the GMS ECM endpoint is vulnerable to XML external entity (XXE) injection vulnerability leading to information disclosure. **CVE-2024-29011** - Use of hard-coded password in the GMS ECM endpoint leading to authentication bypass vulnerability. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SonicWall GMS (Virtual Appliance, Windows) - 9.3.4 and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0007

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5717, CVE-2024-0775, CVE-2024-1086, CVE-2024-26622)
Description	SUSE has released security updates addressing multiple vulnerabilities that exists in SUSE Linux kernel. These vulnerabilities could be exploited by malicious users to cause use-after-free and heap out-of-bounds write conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3 SUSE Linux Enterprise High Performance Computing 15 SP3, 15 SP2 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP2 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Server 15 SP3, 15 SP2 SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241581-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241580-1/

Affected Product	**WordPress**
Severity	**High**
Affected Vulnerability	Cross-Site Scripting Vulnerability
Description	WordPress has released security updates addressing a Cross-Site Scripting Vulnerability that exists in their platform. WordPress Core is vulnerable to Stored Cross-Site Scripting via user display names in the Avatar block due to insufficient output escaping on the display name. WordPress advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WordPress versions prior to 6.5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wordpress.org/news/2024/04/wordpress-6-5-2-maintenance-and-security-release/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-13224, CVE-2019-16163, CVE-2019-19012, CVE-2019-19203, CVE-2019-19204, CVE-2018-19787, CVE-2021-43818, CVE-2014-3146, CVE-2020-27783, CVE-2007-4559, CVE-2022-48560, CVE-2022-48564, CVE-2022-28388, CVE-2022-3545, CVE-2022-3594, CVE-2022-36402, CVE-2022-38096, CVE-2022-38457, CVE-2022-40133, CVE-2022-41858, CVE-2022-45869, CVE-2022-45887, CVE-2022-4744, CVE-2023-1382, CVE-2023-2166, CVE-2023-2176, CVE-2023-28772, CVE-2023-30456, CVE-2023-31084, CVE-2023-33951, CVE-2023-33952, CVE-2023-40283, CVE-2023-45862, CVE-2023-4921, CVE-2023-51042, CVE-2023-51043, CVE-2023-5633, CVE-2023-6606, CVE-2023-6610, CVE-2023-6817, CVE-2023-6931, CVE-2023-7192, CVE-2024-0565, CVE-2024-0646, CVE-2024-1086, CVE-2022-48624, CVE-2023-46218, CVE-2023-38546, CVE-2023-1786, CVE-2021-33631, CVE-2023-6546, CVE-2023-1989, CVE-2023-1998, CVE-2023-23455, CVE-2023-2513, CVE-2023-26545, CVE-2023-28328, CVE-2023-3141, CVE-2023-31436, CVE-2023-3161, CVE-2023-3212, CVE-2023-3268, CVE-2023-33203, CVE-2023-35823, CVE-2023-35824, CVE-2023-3609, CVE-2023-3611, CVE-2023-3772, CVE-2023-4128, CVE-2023-4132, CVE-2023-4155, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-4732, CVE-2023-52425, CVE-2024-1488, CVE-2019-8675, CVE-2019-8696, CVE-2020-3898, CVE-2023-32324, CVE-2023-34241, CVE-2020-10001, CVE-2022-26691, CVE-2023-32360, CVE-2023-46120)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Privilege Escalation, Sensitive Information Disclosure, Code Execution, Cross-Site Scripting. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP8 and UP8 IF01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7150684 • https://www.ibm.com/support/pages/node/7150686

Affected Product	**PostgreSQL**
Severity	**Low**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2024-4317)
Description	PostgreSQL has released security updates addressing a Privilege Escalation Vulnerability that exists in PostgreSQL core server. Missing authorization in PostgreSQL built-in views pg_stats_ext and pg_stats_ext_exprs allows an unprivileged database user to read most common values and other statistics from [CREATE STATISTICS] commands of other users. The most common values may reveal column values the eavesdropper could not otherwise read or results of functions they cannot execute. PostgreSQL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PostgreSQL 14 PostgreSQL 15 PostgreSQL 16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.postgresql.org/support/security/CVE-2024-4317/

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.