Advisory Alert

Alert Number: **AAA20240215** **Date:** **February 15, 2024**

Document Classification Level	:	Public Circulation Permitted | Public
Information Classification Level	:	TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
F5	**High, Medium**	Multiple Vulnerabilities
Node.js	**High, Medium, Low**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities
Palo Alto	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2021-33631, CVE-2023-46838, CVE-2023-47233, CVE-2023-4921, CVE-2023-51043, CVE-2023-51780, CVE-2023-51782, CVE-2023-6040, CVE-2023-6356, CVE-2023-6535, CVE-2023-6536, CVE-2023-6915, CVE-2024-0565, CVE-2024-0775, CVE-2024-1086, CVE-2024-0340, CVE-2024-0641, CVE-2024-1085, CVE-2024-24860)
Description	SUSE has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to privilege escalation, information leak, integer overflow, out-of-bounds access, use-after-free vulnerabilities. SUSE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.3, 15.5 openSUSE Leap Micro 5.3, 5.4 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Availability Extension 15 SP3 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5 SUSE Linux Enterprise Micro for Rancher 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 12 SP5, 15 SP4, 15 SP5 SUSE Linux Enterprise Server 12 SP5, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux 15-SP3 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP4, 15 SP5 SUSE Manager Proxy 4.2 SUSE Manager Retail Branch Server 4.2 SUSE Manager Server 4.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20240474-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240476-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240463-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240468-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240469-1/

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21789, CVE-2024-23607)
Description	F5 has released a security update addressing Multiple Vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to directory traversal and denial-of-service **CVE-2024-21789** - When a BIG-IP Advanced WAF/ASM security policy is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization to cause denial-of-service. **CVE-2024-23607** - A directory traversal vulnerability exists in the F5OS QKView utility that allows an authenticated attacker to read files outside the QKView directory. F5 recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	BIG-IP (Advanced WAF/ASM) - 17.x 17.1.0 F5OS-A 1.x 1.3.0 - 1.3.2 QKView utility F5OS-C 1.x 1.3.0 - 1.5.1 QKView utility
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000132800 https://my.f5.com/manage/s/article/K000137270

Affected Product	**Node.js**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21890 ,CVE-2024-21891, CVE-2023-46809, CVE-2024-22017, CVE-2024-21896, CVE-2024-22019, CVE-2024-21892, CVE-2024-24758, CVE-2024-24806)
Description	Node.js has released a security update addressing Multiple Vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Code injection , privilege escalation, denial of service, Path traversal Node.js recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Node.js active release lines: 18.x, 20.x, and 21.x.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/february-2024-security-releases

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45857, CVE-2023-44270, CVE-2022-25883, CVE-2023-26159, CVE-2023-45133, CVE-2022-43552, CVE-2023-44981, CVE-2023-5676, CVE-2023-43642, CVE-2023-32360, CVE-2022-40982, CVE-2023-3611, CVE-2023-3776, CVE-2023-4128, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-20593, CVE-2023-20569, CVE-2023-37920, CVE-2020-19909, CVE-2023-38546, CVE-2023-38545, CVE-2023-5678, CVE-2023-46218, CVE-2023-46219, CVE-2023-4807, CVE-2024-0727, CVE-2023-6129, CVE-2023-5363, CVE-2024-20918, CVE-2024-20952, CVE-2024-20921, CVE-2024-20945, CVE-2023-33850)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in IBM QRadar and IBM WebSphere Application Server. If exploited these vulnerabilities could lead to denial of service, obtain sensitive information, privilege escalation, arbitrary code execution vulnerabilities. It is recommended by IBM to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM QRadar SIEM 7.5 - 7.5.0 UP7 QRadar WinCollect Agent 10.0-10.1.8 Use Case Manager App 1.0 - 3.8.0 IBM WebSphere Application Server 8.5 IBM WebSphere Application Server 9.0 IBM WebSphere Application Server Liberty Continuous delivery
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7117881 https://www.ibm.com/support/pages/node/7117883 https://www.ibm.com/support/pages/node/7117884 https://www.ibm.com/support/pages/node/7117872

Affected Product	**Palo Alto**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-0007, CVE-2024-0008, CVE-2024-0009, CVE-2024-0010, CVE-2024-0011)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exists in their products. If exploited these vulnerabilities could lead to Stored Cross-Site Scripting, Insufficient Session Expiration , Improper IP Address Verification, Reflected Cross-Site Scripting, It is recommended by Palo Alto to apply necessary security fixes at earliest to avoid issues.
Affected Products	PAN-OS 10.0 versions before 10.0.13 PAN-OS 10.0 versions before 10.0.11 on Panorama PAN-OS 10.0 versions before 10.0.12-h1 PAN-OS 10.1 versions before 10.1.10-h1 PAN-OS 10.1 versions before 10.1.11-h1 PAN-OS 10.1 versions before 10.1.12 PAN-OS 10.1 versions before 10.1.6 on Panorama PAN-OS 10.2 versions before 10.2.5 PAN-OS 11.0 versions before 11.0.2 PAN-OS 8.1 versions before 8.1.24 PAN-OS 8.1 versions before 8.1.24-h1 on Panorama, versions before 8.1.25 on Panorama PAN-OS 9.0 versions before 9.0.17 on Panorama PAN-OS 9.0 versions before 9.0.17-h2, versions before 9.0.18 PAN-OS 9.0 versions before 9.0.17-h4 PAN-OS 9.1 versions before 9.1.16 on Panorama PAN-OS 9.1 versions before 9.1.17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2024-0007 https://security.paloaltonetworks.com/CVE-2024-0008 https://security.paloaltonetworks.com/CVE-2024-0009 https://security.paloaltonetworks.com/CVE-2024-0010 https://security.paloaltonetworks.com/CVE-2024-0011

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.