Advisory Alert

Alert Number: AAA20240119 **Date:** January 19, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Weak Folder Permission Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Lenovo	**High**, **Medium**	Multiple Vulnerabilities
WatchGuard	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Weak Folder Permission Vulnerabilities(CVE-2024-22428)
Description	Dell has released a security update addressing Weak Folder Permission Vulnerabilities that exist in their iDRAC Service Module. These vulnerabilities could be exploited by malicious users to compromise the affected system. **CVE-2024-22428 -** Dell iDRAC Service Module, versions 5.2.0.0 and prior, contain an Incorrect Default Permissions vulnerability. It may allow a local unprivileged user to escalate privileges and execute arbitrary code on the affected system. Dell recommends customers upgrade at the earliest opportunity. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	iDRAC Service Module iSM 5.2.0.0 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000221129/dsa-2024-018-security-update-for-dell-idrac-service-module-for-weak-folder-permission-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2020-26555, CVE-2023-51779, CVE-2023-6121, CVE-2023-6606, CVE-2023-6610, CVE-2023-6931, CVE-2023-6932)
Description	SUSE has released security updates addressing multiple vulnerabilities in the SUSE Linux Kernel. If exploited, these vulnerabilities could lead to escalation of privilege, information leakage, user-after-free condition, out-of-bounds read. SUSE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SUSE Linux Enterprise High Availability Extension 15 SP2, 15 SP3 SUSE Linux Enterprise High Performance Computing 15 SP2, 15 SP2 LTSS 15-SP2, 15 SP3, LTSS 15 SP3 SUSE Linux Enterprise Live Patching 15-SP2, 15-SP3 SUSE Linux Enterprise Server 15 SP2, 15 SP2 LTSS 15-SP2, 15 SP2 Business Critical Linux 15-SP2, 15 SP3, 15 SP3 LTSS 15-SP3, 15 SP3 Business Critical Linux 15-SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP2, 15 SP3 SUSE Manager Proxy 4.1, 4.2 SUSE Manager Retail Branch Server 4.1, 4.2 SUSE Manager Server 4.1, 4.2 openSUSE Leap 15.3 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Micro for Rancher 5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20240154-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240153-1/

Affected Product	**Lenovo**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2023-20593, CVE-2021-26354, CVE-2021-26371, CVE-2021-26391, CVE-2021-26392, CVE-2021-46760, CVE-2021-46773, CVE-2021-46756, CVE-2021-46753, CVE-2021-46754, CVE-2021-26365, CVE-2021-26356, CVE-2021-26393, CVE-2021-26406, CVE-2021-46749, CVE-2021-46755, CVE-2021-46792, CVE-2021-46794, CVE-2021-46765, CVE-2021-46759, CVE-2021-26379, CVE-2021-26397, CVE-2022-23818, CVE-2023-20520, CVE-2023-20524, CVE-2023-27373, CVE-2022-33894, CVE-2022-38087, CVE-2022-48181, CVE-2022-48188, CVE-2023-22614, CVE-2023-22616, CVE-2023-22613, CVE-2023-22615, CVE-2023-22612, CVE-2022-24350, CVE-2022-32471, CVE-2022-32475, CVE-2022-32470, CVE-2022-32469, CVE-2022-32477, CVE-2022-32473, CVE-2022-32476, CVE-2022-32472, CVE-2022-32478, CVE-2022-32474, CVE-2022-32953, CVE-2022-32954, CVE-2022-32955, CVE-2022-32952, CVE-2022-32951, CVE-2022-33972)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exists in third party products that in turn affect Lenovo products. If exploited these could allow a remote attacker to cause Privilege Elevation, Information disclosure, Arbitrary code execution and Denial of Service. It is recommended by Lenovo to apply necessary security fixes at earliest to avoid issues
.Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-130057 https://support.lenovo.com/us/en/product_security/LEN-124495 https://support.lenovo.com/us/en/product_security/LEN-115634 https://support.lenovo.com/us/en/product_security/LEN-107840

Affected Product	**WatchGuard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2023-6332, CVE-2023-6331, CVE-2023-6330)
Description	WatchGuard has released security updates addressing multiple vulnerabilities that exists in their endpoint products. If exploited by the attacker, it could lead to disclosure of Sensitive information, Denial of service, Privilege Elevation. It is recommended by WatchGuard to apply necessary security fixes at earliest to avoid issues
.Affected Products	WatchGuard EPDR and Panda AD360 up to 8.00.22.0023 Panda Dome up to 22.02.01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00003 https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00002 https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00001

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2022-30631, CVE-2018-14041, CVE-2018-20676, CVE-2018-20677, CVE-2023-2801, CVE-2023-44487, CVE-2022-43552, CVE-2023-4813, CVE-2022-39324, CVE-2023-46159, CVE-2023-2183, CVE-2023-1410, CVE-2023-32681, CVE-2023-27538)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in Golang which is used by IBM Storage Ceph. If exploited these could allow a remote attacker to cause Cross-site scripting, Sensitive information disclosure, Denial of service and URL spoofing. It is recommended by IBM to apply necessary security fixes at earliest to avoid issues
.Affected Products	IBM Storage Ceph versions prior to 6.1z3 IBM Storage Ceph versions prior to 5.3z5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7105568 https://www.ibm.com/support/pages/node/7109097 https://www.ibm.com/support/pages/node/7109102 https://www.ibm.com/support/pages/node/7109098 https://www.ibm.com/support/pages/node/7109099 https://www.ibm.com/support/pages/node/7109100 https://www.ibm.com/support/pages/node/7109095 https://www.ibm.com/support/pages/node/7108974 https://www.ibm.com/support/pages/node/7108973 https://www.ibm.com/support/pages/node/7109101 https://www.ibm.com/support/pages/node/7109103 https://www.ibm.com/support/pages/node/7109104 https://www.ibm.com/support/pages/node/7109105 https://www.ibm.com/support/pages/node/7109109 https://www.ibm.com/support/pages/node/7105568

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.