Advisory Alert

Alert Number: AAA20240507 **Date:** May 7, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Lenovo	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5717, CVE-2024-0775, CVE-2024-1086, CVE-2023-51775)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Heap out-of-bounds write, Denial of Service, Use-After-Free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4, 15.5 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP2, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15 SP2, 15 SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 12 SP5, 15 SP2, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP2, 15 SP5 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241491-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241493-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241505-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241506-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241532-1/

Affected Product	**Dell**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2014-3577, CVE-2012-5783, CVE-2020-13956, CVE-2012-6153, CVE-2015-5262, CVE-2023-46589, CVE-2023-24932)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products that in turn affect Dell NetWorker. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell NetWorker - NetWorker Server - Versions 19.9 through 19.9.0.5, Versions 19.8 through 19.8.0.4 and Versions 19.8 prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000224800/dsa-2024-208-security-update-for-dell-networker-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000224798/dsa-2024-207-security-update-for-dell-networker-for-bmr-iso-vulnerability

Affected Product	**Lenovo**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-34884, CVE-2022-34888, CVE-2023-4606, CVE-2023-4607, CVE-2023-4608)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exists their products. Exploitation of these vulnerabilities may lead to Denial of Service, Data Tampering, Privilege Escalation and Information Disclosure. Lenovo 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://support.lenovo.com/us/en/product_security/LEN-87734 • https://support.lenovo.com/us/en/product_security/LEN-140960

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.