Advisory Alert

Alert Number: AAA20240614 **Date:** June 14, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2016-9566, CVE-2019-3698, CVE-2019-14889, CVE-2020-1730, CVE-2021-3634, CVE-2023-2283, CVE-2023-6004, CVE-2023-6918, CVE-2019-25162, CVE-2020-36777, CVE-2020-36784, CVE-2021-46906, CVE-2021-46915, CVE-2021-46921, CVE-2021-46924, CVE-2021-46929, CVE-2021-46932, CVE-2021-46953, CVE-2021-46974, CVE-2021-46991, CVE-2021-46992, CVE-2021-47013, CVE-2021-47054, CVE-2021-47076, CVE-2021-47077, CVE-2021-47078, CVE-2022-20154, CVE-2022-48627, CVE-2023-28746, CVE-2023-35827, CVE-2023-46343, CVE-2023-52340, CVE-2023-52429, CVE-2023-52445, CVE-2023-52449, CVE-2023-52451, CVE-2023-52464, CVE-2023-52475, CVE-2023-52478, CVE-2023-52482, CVE-2023-52502, CVE-2023-52530, CVE-2023-52531, CVE-2023-52532, CVE-2023-52574, CVE-2023-52597, CVE-2023-52605, CVE-2024-0607, CVE-2024-1086, CVE-2024-1151, CVE-2024-23849, CVE-2024-23851, CVE-2024-26585, CVE-2024-26595, CVE-2024-26600, CVE-2024-26622, CVE-2022-1996, CVE-2022-28737, CVE-2023-40546, CVE-2023-40547, CVE-2023-40548, CVE-2023-40549, CVE-2023-40550, CVE-2023-40551, CVE-2022-48624, CVE-2024-32487, CVE-2023-4750, CVE-2023-48231, CVE-2023-48232, CVE-2023-48233, CVE-2023-48234, CVE-2023-48235, CVE-2023-48236, CVE-2023-48237, CVE-2023-48706, CVE-2024-22667, CVE-2023-7207, CVE-2023-38709, CVE-2024-24795, CVE-2024-27316, CVE-2023-42465, CVE-2023-45918, CVE-2023-51385, CVE-2023-51767, CVE-2024-0727, CVE-2024-2511, CVE-2024-1597, CVE-2024-2004, CVE-2024-2398, CVE-2024-2961, CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-22243, CVE-2024-22259, CVE-2024-23651, CVE-2024-23652, CVE-2024-23653, CVE-2024-23672, CVE-2024-24549, CVE-2024-25062, CVE-2024-25710, CVE-2024-26458, CVE-2024-26461, CVE-2024-28085, CVE-2024-28182, CVE-2024-30172, CVE-2023-33202, CVE-2024-20923, CVE-2024-20926, CVE-2024-20932, CVE-2024-22234, CVE-2024-22257, CVE-2024-22262, CVE-2024-0340, CVE-2024-0775, CVE-2023-42282, CVE-2023-22467, CVE-2022-3517, CVE-2022-46175, CVE-2022-25881, CVE-2024-37131)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. 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 Secure Connect Gateway - Version 5.22.00.18 Dell Policy Manager for Secure Connect Gateway - 5.18.20 through 5.22.00.18
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000225991/dsa-2024-253-dell-secure-connect-gateway-security-update-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000225956/dsa-2024-254-security-update-for-dell-secure-connect-gateway-policy-manager-vulnerabilities

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 Use After Free, NULL Pointer Dereference, Memory Leak, Out Of Bounds Access. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.5 Public Cloud Module 15-SP5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20242019-1

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.