Advisory Alert

Alert Number: AAA20240624 **Date:** June 24, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NETGEAR	**High**	SQL Injection Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**NETGEAR**
Severity	**High**
Affected Vulnerability	SQL Injection Vulnerabilities
Description	NETGEAR has released security updates addressing SQL Injection Vulnerabilities that exist on the Prosafe Network Management System (NMS300). NETGEAR advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NMS300 software version prior to 1.7.0.37
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://kb.netgear.com/000066231/Security-Advisory-for-SQL-Injection-on-the-NMS300-PSV-2024-0018?_ga=2.128311375.210285148.1719203804-509677121.1718854234 • https://kb.netgear.com/000066232/Security-Advisory-for-SQL-Injection-on-the-NMS300-PSV-2024-0019?_ga=2.128311375.210285148.1719203804-509677121.1718854234

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237, CVE-2022-36765)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Code Execution, Denial of Service (DoS), Disclosure of Information, local buffer overflow. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Compute Scale-up Server 3200 - Prior to v1.20.128 HPE Superdome Flex 280 Server - Prior to v1.80.20 HPE Superdome Flex Server - Prior to v3.100.26
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04576en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04632en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing Multiple Vulnerabilities that exist in third-party products that in turn affect dell 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 EMC VxRail Appliance 7.0.x versions prior to 7.0.520
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000226270/dsa-2024-247-security-update-for-dell-vxrail-7-0-520-multiple-third-party-component-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 compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.3, 15.4, 15.6 Public Cloud Module 15-SP6 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP2, 15 SP3, 15 SP4 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP2, 15-SP3, 15-SP4 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 12 SP5, 15 SP2, 15 SP3, 15 SP4, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP2, 15 SP3, 15 SP4, 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242109-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242115-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242120-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242121-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242123-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242124-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242130-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242135-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242139-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242143-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242145-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242147-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242148-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242149-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242156-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242160-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242162-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242163-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242164-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242165-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242166-1

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51043, CVE-2024-1086, CVE-2024-0646, CVE-2023-6932, CVE-2024-26582, CVE-2023-6817, CVE-2024-20952, CVE-2024-20918, CVE-2024-20921, CVE-2024-20919, CVE-2024-20926, CVE-2024-20945, CVE-2023-33850)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Storage Scale and IBM Storage Insights. These vulnerabilities could be exploited by malicious users to cause Privilege Escalation, Arbitrary Code Execution, Sensitive Information Disclosure, high confidentiality and integrity impact. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale System versions 6.1.0.0 - 6.1.2.9 and 6.1.3.0 - 6.1.9.2 IBM Storage Insights - Data Collector 20240510-0638 and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7158270 • https://www.ibm.com/support/pages/node/7158490

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.