TLP: WHITE

Advisory Alert

Alert Number: **AAA20240712** **Date:** **July 12, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Remote Code Execution Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Citrix	**High**	Privilege Escalation Vulnerability
IBM	**High**	Remote Code Execution Vulnerability
Suse	**High**	Multiple Vulnerabilities
Ubuntu	**High, Medium, Low**	Multiple Vulnerabilities
Hitachi	**High, Medium, Low**	Multiple Vulnerabilities
NetApp	**High, Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2023-46604)
Description	NetApp has released security updates addressing a Remote Code Execution vulnerability that exists in Apache ActiveMQ third-party products that in turn affect netapp products. If exploited, this vulnerability could lead to Denial of Service, Modification of Data, Sensitive Information Disclosure. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	E-Series SANtricity Unified Manager and Web Services Proxy SANtricity Storage Plugin for vCenter
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20231110-0010/

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party components which 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 - 8.0.x versions prior to 8.0.213
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000226863/dsa-2024-289-security-update-for-dell-vxrail-8-0-213-multiple-third-party-component-vulnerabilities

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2024-6677)
Description	Citrix has released security updates addressing a privilege escalation vulnerability that exists in the Citrix uberAgent. This vulnerability is caused due to a system PATH environment variable includes a directory that is writable by users. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Citrix uberAgent before 7.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX691103/citrix-uberagent-security-bulletin-for-cve20246677

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2024-35154)
Description	IBM has released security updates addressing a Remote Code Execution Vulnerability that exists in IBM products. IBM WebSphere Application Server which is bundled with IBM WebSphere Hybrid Edition, could allow a remote authenticated attacker, who has authorized access to the administrative console, to execute arbitrary code. Using specially crafted input, the attacker could exploit this vulnerability to execute arbitrary code on the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Hybrid Edition - Version 5.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7160014

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26828, CVE-2024-26923)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Arbitrary code execution and Privilege escalation. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 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-20242407-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242410-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242411-1

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6893-1

Affected Product	**Hitachi**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26238, CVE-2024-29994, CVE-2024-29996, CVE-2024-29997, CVE-2024-29998, CVE-2024-29999, CVE-2024-30000, CVE-2024-30001, CVE-2024-30002, CVE-2024-30003, CVE-2024-30004, CVE-2024-30005, CVE-2024-30006, CVE-2024-30008, CVE-2024-30009, CVE-2024-30012, CVE-2024-30014, CVE-2024-30015, CVE-2024-30016, CVE-2024-30017, CVE-2024-30018, CVE-2024-30020, CVE-2024-30021, CVE-2024-30022, CVE-2024-30023, CVE-2024-30024, CVE-2024-30025, CVE-2024-30027, CVE-2024-30028, CVE-2024-30029, CVE-2024-30031, CVE-2024-30032, CVE-2024-30033, CVE-2024-30034, CVE-2024-30035, CVE-2024-30037, CVE-2024-30038, CVE-2024-30039, CVE-2024-30040, CVE-2024-30049, CVE-2024-30050, CVE-2024-30051)
Description	Hitachi has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Remote Code Execution, Information Disclosure, Privilege Escalation, Security Feature Bypass Hitachi advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform 5100, 5200, 5500,5600, 5100H, 5200H, 5600H, 5500H, G1000, G1500, F1500, VX7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2024/05.html

Affected Product	**NetApp**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-20922, CVE-2024-20923, CVE-2024-20925, CVE-2024-20926, CVE-2024-20932, CVE-2024-20945, CVE-2024-20952, CVE-2023-33202, CVE-2023-26049, CVE-2023-26048, CVE-2023-24998, CVE-2020-27223, CVE-2024-6387, CVE-2024-24788, CVE-2023-45288, CVE-2023-45289, CVE-2024-25710, CVE-2024-26308, CVE-2022-41678)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Disclosure of Sensitive Information, Denial of Service, Addition or Modification of Data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9 all Versions if the LoginGraceTime value is not set to 0. E-Series SANtricity OS Controller Software 11.x with SSH login disabled SnapManager for SAP SnapManager for Oracle SnapCenter Snap Creator Framework SANtricity Storage Plugin for vCenter NetApp BlueXP Management Services for Element Software and NetApp HCI E-Series SANtricity Unified Manager and Web Services Proxy E-Series SANtricity OS Controller Software 11.x Element Plug-in for vCenter Server Cloud Insights Storage Workload Security Agent Cloud Insights Acquisition Unit Astra Trident Active IQ Unified Manager for VMware vSphere Active IQ Unified Manager for Microsoft Windows Active IQ Unified Manager for Linux
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20240701-0001/ • https://security.netapp.com/advisory/ntap-20240605-0002/ • https://security.netapp.com/advisory/ntap-20240419-0009/ • https://security.netapp.com/advisory/ntap-20240329-0006/ • https://security.netapp.com/advisory/ntap-20240307-0010/ • https://security.netapp.com/advisory/ntap-20240307-0009/ • https://security.netapp.com/advisory/ntap-20240216-0004/ • https://security.netapp.com/advisory/ntap-20240201-0002/ • https://security.netapp.com/advisory/ntap-20240125-0001/ • https://security.netapp.com/advisory/ntap-20231110-0010/ • https://security.netapp.com/advisory/ntap-20230526-0001/ • https://security.netapp.com/advisory/ntap-20230302-0013/ • https://security.netapp.com/advisory/ntap-20210401-0005/

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.