Advisory Alert

Alert Number: **AAA20230810** **Date:** **August 10, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Sensitive Information Disclosure Vulnerability
Lenovo	**High**	Multiple Vulnerabilities
Dell	**Medium**	Privilege Escalation Vulnerability
Fortinet	**Medium**	Stack-based buffer overflow Vulnerability

Description

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Sensitive Information Disclosure Vulnerability (CVE-2023-33201)
Description	IBM Storage Scale contains a Sensitive Information Disclosure vulnerability caused by not validating the X.500 name of any certificate in the implementation of the X509LDAPCertStoreSpi.java class. By exploiting this vulnerability a remote authenticated user can execute commands and launch further attacks against the affected system. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Storage Scale 5.1.0.0 - 5.1.2.11 IBM Storage Scale 5.1.3.0 - 5.1.8.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7022431

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3602, CVE-2022-3786, CVE-2022-27635, CVE-2022-46329, CVE-2022-40964, CVE-2022-36351, CVE-2022-38076, CVE-2022-36392, CVE-2022-38102, CVE-2022-29871, CVE-2022-24351, CVE-2022-27879, CVE-2022-37343, CVE-2022-38083, CVE-2022-40982, CVE-2022-41804, CVE-2022-43505, CVE-2022-44611, CVE-2022-46897, CVE-2023-2004, CVE-2023-20555, CVE-2023-20569, CVE-2023-23908, CVE-2023-26090, CVE-2023-27471, CVE-2023-28468, CVE-2023-31041, CVE-2023-34419, CVE-2023-4028, CVE-2023-4029, CVE-2023-4030)
Description	Lenovo has released a security update addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Denial of Service, Information Disclosure, Privilege escalation and Remote code execution. Lenovo recommends to apply the necessary security updates 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-106015 https://support.lenovo.com/us/en/product_security/LEN-115701 https://support.lenovo.com/us/en/product_security/LEN-121185 https://support.lenovo.com/us/en/product_security/LEN-134879

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2021-41526)
Description	Dell has released security updates addressing a Privilege Escalation vulnerability affecting their third-Party Components. Dell recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	(Dell System Update) DSU versions prior to 2.0.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000216605/dsa-2023-280-dell-system-update-dsu-security-update-for-a-privilege-escalation-vulnerability

Affected Product	**Fortinet**
Severity	**Medium**
Affected Vulnerability	Stack-based buffer overflow Vulnerability (CVE-2023-29182)
Description	Fortinet has released a security update addressing a Stack-based buffer overflow vulnerability that exist in FortiOS. Successful exploitation of this vulnerability may allow a privileged attacker to execute arbitrary code via specially crafted CLI commands Fortinet recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	FortiOS version 7.0.0 through 7.0.3 FortiOS 6.4 all versions FortiOS 6.2 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-149

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.