Advisory Alert

Alert Number: AAA20230512 **Date:** May 12, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Lenovo	**High**	Multiple Vulnerabilities
NetApp	**High**	Authentication Bypass Vulnerability
Intel	**High**, **Medium**	Multiple Vulnerabilities
IBM	**Medium**	XML External Entity (XXE) Injection vulnerability
Redhat	**Medium**	Information Disclosure Vulnerability

Description

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26354, CVE-2021-26356, CVE-2021-26365, CVE-2021-26371, CVE-2021-26379, CVE-2021-26391, CVE-2021-26392, CVE-2021-26393, CVE-2021-26397, CVE-2021-26406, CVE-2021-46749, CVE-2021-46753, CVE-2021-46754, CVE-2021-46755, CVE-2021-46756, CVE-2021-46759, CVE-2021-46762, CVE-2021-46763, CVE-2021-46764, CVE-2021-46765, CVE-2021-46769, CVE-2021-46773, CVE-2021-46775, CVE-2021-46792, CVE-2021-46794, CVE-2022-23818, CVE-2022-33894, CVE-2022-38087, CVE-2022-4569,CVE-2022-48181, CVE-2022-48188,CVE-2023-20520, CVE-2023-20524, CVE-2023-27373, CVE-2023-29552)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of the vulnerabilities could lead to Denial of Service, Privilege Elevation and Information Disclosure Lenovo recommends to apply the necessary patch updates at your 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-103544 https://support.lenovo.com/us/en/product_security/LEN-124495 https://support.lenovo.com/us/en/product_security/LEN-123896

Affected Product	**NetAPP**
Severity	**High**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2023-1096)
Description	NetAPP has released a security update addressing a Privilege Escalation vulnerability that exists in NetApp SnapCenter **CVE-2023-1096** - SnapCenter versions 4.7 prior to 4.7P2 and 4.8 prior to 4.8P1 are susceptible to a vulnerability which could allow a remote unauthenticated attacker to gain access as an admin user. NetApp recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SnapCenter versions 4.7 prior to 4.7P2 and 4.8 prior to 4.8P
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20230511-0011/

Affected Product	**Intel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-28699, CVE-2022-31477, CVE-2022-32577, CVE-2022-32582, CVE-2022-32766, CVE-2022-33894, CVE-2022-34147, CVE-2022-36339, CVE-2022-37327, CVE-2022-38087, CVE-2022-38101, CVE-2022-38787, CVE-2023-22312, CVE-2023-22379, CVE-2023-22443, CVE-2023-24475, CVE-2023-25175, CVE-2023-25771, CVE-2023-25776, CVE-2023-28411)
Description	Intel has released a security updates addressing multiple vulnerabilities that exist in the Firmware and BIOS of their products. Exploitation of the vulnerabilities could lead to Privilege Escalation, Denial of Service and Information Disclosure. Intel recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00839.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00824.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00807.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00780.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00777.html

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	XML External Entity (XXE) Injection vulnerability (CVE-2023-27554)
Description	IBM has released a security updates addressing an XML External Entity (XXE) Injection vulnerability that exist in their products. **CVE-2023-27554** - A XML External Entity Injection Vulnerability that exists in IBM WebSphere Application Server when processing data. A remote attacker can exploit this vulnerability to expose sensitive information or consume memory resources. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Maximo Asset Management 7.6.1.2 - 7.6.1.3 IBM WebSphere Application Server 8.5.5 Full Profile IBM WebSphere Application Server 8.5 - 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6989657 https://www.ibm.com/support/pages/node/6989665

Affected Product	**Redhat**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2021-0341)
Description	Redhat has released a security update addressing an Information Disclosure Vulnerability that exist in their products **CVE-2021-0341** - In verifyHostName of OkHostnameVerifier.java, there is a possible way to accept a certificate for the wrong domain due to improperly used crypto. This could lead to remote information disclosure with no additional execution privileges needed. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat JBoss Data Grid Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:2723

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.