TLP: WHITE

Advisory Alert

Alert Number: **AAA20231002** **Date:** **October 2, 2023**

Document Classification Level	:	Public Circulation Permitted | Public
Information Classification Level	:	TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Arbitrary Code Execution Vulnerabilities
Ubuntu	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Dell	**High**	An Improper Access Control Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities
Watchguard	**High**, **Medium**	Multiple Vulnerabilities
Trellix	**Medium**	Privilege Escalation Vulnerability
Redhat	**Medium**	Multiple Vulnerabilities
Netapp	**Medium**	Multiple Denial Of Service Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Arbitrary Code Execution Vulnerabilities
Description	IBM has released security updates addressing multiple critical Arbitrary code execution vulnerabilities that exist in their products. IBM highly recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	IBM Disconnected Log Collector v1.0 - v1.8.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7042313

Affected Product	**Ubuntu**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4128, CVE-2023-20588, CVE-2023-40283, CVE-2023-4569)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to sensitive Information disclosure, denial of service, arbitrary code execution Ubuntu recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6386-2

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1829, CVE-2023-31248, CVE-2023-3609, CVE-2023-3776, CVE-2023-3812, CVE-2023-4273)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to use-after-free condition, reference counter leakage, System crash, Privilege Escalation. Suse recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	SUSE Linux Enterprise High Performance Computing 15 SP2, 15 SP3 SUSE Linux Enterprise Live Patching 15-SP2, 15-SP3 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Server 15 SP2, 15 SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP2, 15 SP3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233892-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233891-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233889-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233893-1

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	An Improper Access Control Vulnerability (CVE-2023-32477)
Description	Dell has released security updates addressing an Improper access control vulnerability. Exploitation of this vulnerability may lead to privilege escalation. Dell highly recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Dell EMC Common Event Enabler Windows CEE versions prior to CEE 8.9.9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000218120/dsa-2023-310-security-update-for-dell-emc-common-event-enabler

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple that exist in their products. Successful exploitation of these vulnerabilities may lead to Denial of service, Sensitive information disclosure, Path traversal, Arbitrary code execution. IBM highly recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	IBM Disconnected Log Collector v1.0 - v1.8.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7042313

Affected Product	**Watchguard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-26236, CVE-2023-26237, CVE-2023-26238, CVE-2023-26239)
Description	Watchguard has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Privilege Escalation, Advanced Protection Bypass, Anti-Tamper Protection Bypass and Information Disclosure. Watchguard recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	WatchGuard EPDR and Panda AD360 versions before 8.00.22.0010
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2023-00007 https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2023-00006 https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2023-00005 https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2023-00004

Affected Product	**Trellix**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability(CVE-2023-4814)
Description	Trellix has released security updates addressing a Privilege escalation vulnerability exists in Trellix Windows DLP endpoint for windows. Successful exploitation could lead to deletion of any file/folder for which the user does not have permission to. Trellix recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Trellix Data Loss Prevention Endpoint (DLP) version 11.10.100.17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kcm.trellix.com/corporate/index?page=content&id=SB10407&actp=null&viewlocale=en_US&showDraft=false&platinum_status=false&locale=en_GB

Affected Product	**Redhat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-45047, CVE-2023-3628, CVE-2023-3629, CVE-2023-5236, CVE-2023-34462, CVE-2023-35116, CVE-2023-35887)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Denial of service, Information disclosure, Out of memory errors, Privilege escalation. Redhat recommends to apply the necessary security updates at 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-2023:5396

Affected Product	**Netapp**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-4269, CVE-2023-2269, CVE-2023-31081, CVE-2023-31082, CVE-2023-31083, CVE-2023-31084, CVE-2023-31085)
Description	Netapp has released security updates addressing multiple Denial of service vulnerabilities that exist in their products. Netapp recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S NetApp HCI Baseboard Management Controller (BMC) - H410C
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20230929-0004/ https://security.netapp.com/advisory/ntap-20230929-0001/ https://security.netapp.com/advisory/ntap-20230929-0003/

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.