Advisory Alert

Alert Number: AAA20221117 **Date:** November 17, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ubuntu	**High**	Multiple Vulnerabilities
Cisco	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Suse	**High**, **Medium**	Multiple Vulnerabilities
Redhat	**Medium**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities
Debian	**Low**	Multiple Vulnerabilities

Description

Affected Product	**Ubuntu**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-41741, CVE-2022-41742, CVE-2020-16845, CVE-2022-40023, CVE-2022-1015, CVE-2022-2602, CVE-2022-41674, CVE-2022-42720, CVE-2022-42721, CVE-2022-42722)
Description	Ubuntu has released a security update addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could cause denial of service and arbitrary memory access. Ubuntu recommends to apply the available patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 22– versions prior to Ubuntu 22.10 Ubuntu 20– versions prior to Ubuntu 20.04 Ubuntu 18– versions prior to Ubuntu 18.04 Ubuntu 16– versions prior to Ubuntu 16.04 Ubuntu 14– versions prior to Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5722-1 https://ubuntu.com/security/notices/USN-5725-1 https://ubuntu.com/security/notices/USN-5625-2 https://ubuntu.com/security/notices/LSN-0090-1

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20964, CVE-2022-20965, CVE-2022-20966, CVE-2022-20967)
Description	Cisco has released a security update to address multiple vulnerabilities that exist in their Service engine. If exploited these vulnerabilities could cause arbitrary command injection, security connection bypass and cross-site scripting Cisco recommends to apply the available patch updates at your earliest to avoid issues.
Affected Products	Cisco ISE Release 2.7 and earlier, 3.02 and earlier, 3.1, 3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-7Q4TNYUx

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-34446, CVE-2022-34447, CVE-2022-34448, CVE-2022-34449, CVE-2022-34450, CVE-2022-34451, CVE-2022-34452)
Description	Dell has released a security update to address multiple vulnerabilities that exist in PowerPath Management Appliance. If exploited, these vulnerabilities could cause privilege escalation, sensitive information discloser and hijack user sessions to send arbitrary requests unknowingly to the server Dell recommends to apply the available patch updates at your earliest to avoid issues.
Affected Products	PowerPath Management Appliance 3.3, 3.2*, 3.1 & 3.0*
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000205404/dsa-2022-283-powerpath-management-appliance-security-update-for-multiple-security-vulnerabilities

Affected Product	**Suse**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-36557, CVE-2020-36558, CVE-2021-33655, CVE-2021-39698, CVE-2021-43980, CVE-2022-1615, CVE-2022-1882, CVE-2022-2255, CVE-2022-24836, CVE-2022-2588, CVE-2022-29181, CVE-2022-33746, CVE-2022-33747, CVE-2022-33748, CVE-2022-36033, CVE-2022-39189, CVE-2022-42309, CVE-2022-42310, CVE-2022-42311, CVE-2022-42312, CVE-2022-42313, CVE-2022-42314, CVE-2022-42315, CVE-2022-42316, CVE-2022-42317, CVE-2022-42318, CVE-2022-42319, CVE-2022-42320, CVE-2022-42321, CVE-2022-42322, CVE-2022-42323, CVE-2022-42325, CVE-2022-42326, CVE-2022-42327, CVE-2022-42703, CVE-2022-42722, CVE-2020-11979, CVE-2020-1945)
Description	Suse has released security updates to address multiple vulnerabilities that exist in their products. If exploited, the most severe vulnerabilities could cause privilege escalation or denial of service. Suse recommends to apply the available patch updates at your earliest to avoid issues.
Affected Products	HPE Helion Openstack 8 openSUSE Leap 15.3,15.4 SUSE Enterprise Storage 6,7,7.1 SUSE Linux Enterprise Desktop 15-SP3, 15-SP4 SUSE Linux Enterprise High Availability 15, 15-SP1, 15-SP2 SUSE Linux Enterprise High Performance Computing 12 SUSE Linux Enterprise High Performance Computing 15, 15-SP1,15-SP2, 15-SP3, 15-SP4 SUSE Linux Enterprise Live Patching 12-SP4, 12-SP5 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Module for Basesystem 15-SP3, 15-SP4 SUSE Linux Enterprise Module for Development Tools 15-SP3, 15-SP4 SUSE Linux Enterprise Module for Live Patching 15, 15-SP1, 15-SP2, 15-SP3, 15-SP4 SUSE Linux Enterprise Software Development Kit 12-SP5 SUSE Linux Enterprise Module for Public Cloud 12, 15-SP4 SUSE Linux Enterprise Module for Web Scripting 12 SUSE Linux Enterprise Server 12, 12-SP3, 12-SP4, 12-SP5 SUSE Linux Enterprise Server 15, 15-SP1, 15-SP2, 15-SP3, 15-SP4 SUSE Linux Enterprise Server for SAP Applications 12, 12-SP3, 12-SP4, 12-SP5 SUSE Linux Enterprise Server for SAP Applications 15, 15-SP1, 15-SP2, 15-SP3, 15-SP4 SUSE Manager Proxy 4.0, 4.1, 4.2, 4.3 SUSE Manager Retail Branch Server 4.0, 4.1, 4.2, 4.3 SUSE Manager Server 4.0, 4.1, 4.2, 4.3 SUSE OpenStack Cloud 8 SUSE OpenStack Cloud Crowbar 8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/

Affected Product	**Redhat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0155, CVE-2022-2805)
Description	Redhat has released a security update to address multiple vulnerabilities that exist in Red Hat Virtualization Manager. **CVE-2022-0155**- A flaw was found in follow-redirects when fetching a remote URL with a cookie when it gets to the Location response header. This flaw allows an attacker to hijack the account as the cookie is leaked. **CVE-2022-2805**- A flaw was found in ovirt-engine, which leads to the logging of plaintext passwords in the log file when using otapi-style. This flaw allows an attacker with sufficient privileges to read the log file, leading to confidentiality loss. Redhat recommends to apply the available patch updates at your earliest to avoid issues.
Affected Products	Red Hat Virtualization Manager 4.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:8502

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-21626 , CVE-2022-21624)
Description	IBM has released a security update to address multiple vulnerabilities that exist in their IBM Java SDK, that affect IBM WebSphere Application Server and IBM WebSphere Application Server Liberty. **CVE-2022-21626**- Java SE contains an unspecific vulnerability related to the Security component that could allow an unauthenticated attacker to cause a denial of service resulting in a low availability impact using unknown attack vectors. **CVE-2022-21624**- Java SE contains an unspecific vulnerability related to the Security component that could allow an unauthenticated attacker to update, insert or delete data resulting in a low integrity impact using unknown attack vectors. IBM recommends to apply the available patch updates at your earliest to avoid issues.
Affected Products	IBM WebSphere Application Server 9.0, 8.5 IBM WebSphere Application Server Liberty Continuous delivery
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6839565

Affected Product	**Debian**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2601, CVE-2022-3775)
Description	Debian has released a security update to address multiple vulnerabilities that exist in their GRUB2 package. **CVE-2022-3775**- Due to a boundary error when rendering certain unicode sequences in grub2 font code. An attacker with physical access to device can crash the system. **CVE-2022-2601**- Due to a boundary error within the grub_font_construct_glyph() function when handling pf2 font. An attacker with physical access to the affected system can bypass implemented security restrictions. Debian recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	grub2 (PTS) 2.06-3~deb10u2 grub2 (PTS) 2.06-3~deb11u4 grub2 (PTS) 2.06-5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.debian.org/lts/security/2022/dla-3190

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.