Advisory Alert

Alert Number: AAA20231122 **Date:** November 22, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
DELL	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities
Dell	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3446, CVE-2022-32148, CVE-2022-32149, CVE-2023-3978, CVE-2023-20569, CVE-2022-40982, CVE-2023-23908, CVE-2023-20900, CVE-2023-28840, CVE-2023-28841, CVE-2023-28842, CVE-2023-4016, CVE-2022-36402, CVE-2023-4752, CVE-2023-4781, CVE-2023-4738, CVE-2023-4735, CVE-2023-4734, CVE-2023-4733, CVE-2023-3341, CVE-2023-34048, CVE-2023-34056)
Description	Dell has released security updates addressing the multiple critical vulnerabilities that exists in third party products that in turn affect Dell products. Exploitation of these vulnerabilities may lead to Denial of Service, Cross-site Scripting, Information disclosure, Privilege escalation. Dell recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	PowerProtect Cyber Recovery 19.14.0.2 and Prior PowerStore 1000X, 3000X, 5000X, 7000X, 9000X
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000219750/dsa-2023-421-security-update-for-dell-powerprotect-cyber-recovery https://www.dell.com/support/kbdoc/en-us/000219749/dsa-2023-433-dell-powerstore-security-update-for-vmware-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-38297, CVE-2020-28367, CVE-2020-28366, CVE-2015-20107)
Description	IBM has released security updates addressing the multiple critical vulnerabilities their products **CVE-2021-38297** - Golang Go is vulnerable to a buffer overflow, caused by improper bounds checking when invoking functions from WASM modules. By passing very large arguments, a remote attacker could overflow a buffer and execute arbitrary code on the system. **CVE-2020-28367** - Golang Go could allow a remote attacker to execute arbitrary code on the system, caused by an argument injection flaw in go command when cgo is in use in build time. By using a specially-crafted package, an attacker could exploit this vulnerability to execute arbitrary code on the system. **CVE-2020-28366** - Golang Go could allow a remote attacker to execute arbitrary code on the system, caused by a code injection flaw in go command when cgo is in use in build time. By using a specially-crafted package, an attacker could exploit this vulnerability to execute arbitrary code on the system. **CVE-2015-20107** - Python could allow a remote attacker to execute arbitrary commands on the system, caused by improper input validation in mailcap module. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	IBM Cloud Pak for Security 1.10.0.0 - 1.10.11.0 QRadar Suite Software 1.10.12.0 - 1.10.16.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7080058

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1829, CVE-2023-3609, CVE-2023-3776, CVE-2023-4004, CVE-2022-40982, CVE-2023-3611, CVE-2023-4128, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-3812, CVE-2023-5178, CVE-2023-42753, CVE-2023-4147, CVE-2023-0590, CVE-2023-20593, CVE-2022-27672)
Description	Red hat has released security updates addressing the multiple vulnerabilities that exists in their products. Exploitation of these vulnerabilities may lead Privilege escalation, System crash, side-channel attack, Information disclosure. Red Hat recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.0 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Power, little endian 7 ppc64le Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.2 x86_64 Red Hat Enterprise Linux for Real Time 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 8.2 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux Workstation 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:7434 https://access.redhat.com/errata/RHSA-2023:7431 https://access.redhat.com/errata/RHSA-2023:7424 https://access.redhat.com/errata/RHSA-2023:7423 https://access.redhat.com/errata/RHSA-2023:7419 https://access.redhat.com/errata/RHSA-2023:7418 https://access.redhat.com/errata/RHSA-2023:7417 https://access.redhat.com/errata/RHSA-2023:7411 https://access.redhat.com/errata/RHSA-2023:7410 https://access.redhat.com/errata/RHSA-2023:7389 https://access.redhat.com/errata/RHSA-2023:7382 https://access.redhat.com/errata/RHSA-2023:7379

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20592, CVE-2023-23583, CVE-2023-0464)
Description	HPE has released security updates addressing the multiple vulnerabilities that exists in their products. **CVE-2023-20592** - A potential security vulnerability has been identified in certain HPE ProLiant DL/DX/XL servers using certain AMD EPYC processors. This vulnerability could be locally exploited to allow memory integrity vulnerability **CVE-2023-23583** - Potential security vulnerabilities have been identified in HPE Edgeline servers. These vulnerabilities could be locally exploited to allow escalation of privilege and/or information disclosure and/or denial of service. **CVE-2023-0464** - A Security vulnerability has been identified in HP-UX OpenSSL A.01.01.01t.001. This vulnerability may cause local and remote denial of service. HPE recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	HPE ProLiant DL325 Gen10 Plus server - Prior to 2.90_10-27-2023 HPE ProLiant DL385 Gen10 Plus server - Prior to 2.90_10-27-2023 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to 2.90_10-27-2023 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to 2.90_10-27-2023 HPE ProLiant DX325 Gen10 Plus v2 server - Prior to 2.90_10-27-2023 HPE ProLiant DX385 Gen10 Plus v2 server - Prior to 2.90_10-27-2023 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to 2.90_10-27-2023 HPE ProLiant XL645d Gen10 Plus Server - Prior to 2.90_10-27-2023 HPE ProLiant XL675d Gen10 Plus Server - Prior to 2.90_10-27-2023 HPE Edgeline e920t Server Blade - Prior to 1.78_10-31-2023 HPE Edgeline e920 Server Blade - Prior to 1.78_10-31-2023 HPE Edgeline e920d Server Blade - Prior to 1.78_10-31-2023 HP-UX OpenSSL Software - Prior to A.01.01.01w.001
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04568en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04554en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbux04564en_us

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3817, CVE-2018-7738, CVE-2023-38039, CVE-2022-48566, CVE-2023-39615, CVE-2023-2454, CVE-2023-2455, CVE-2023-39417, CVE-2023-39418, CVE-2023-41080, CVE-2023-2828, CVE-2023-3341, CVE-2023-21930, CVE-2023-21937, CVE-2023-21938, CVE-2023-21939, CVE-2023-21954, CVE-2023-21967, CVE-2023-21968, CVE-2023-22045, CVE-2023-22049)
Description	Dell has released security updates addressing the multiple vulnerabilities that exists in third party products that in turn affect Dell products. Exploitation of these vulnerabilities may lead to Denial of Service, URL Redirection, Heap Overflow, Privilege escalation. Dell recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Cyber Sense - Index Engines - 8.3 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000219751/dsa-2023-428-security-update-for-dell-index-engines-cybersense

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34104, CVE-2023-41080, CVE-2022-36777, CVE-2021-37713, CVE-2021-37712, CVE-2021-37701, CVE-2021-32804, CVE-2021-32803, CVE-2022-48303, CVE-2022-28327, CVE-2022-24921, CVE-2022-24675, CVE-2022-23806, CVE-2022-23772, CVE-2022-23773, CVE-2022-15586, CVE-2021-44716, CVE-2021-41772, CVE-2021-41771, CVE-2021-39293, CVE-2021-36221, CVE-2021-33198, CVE-2021-33197, CVE-2021-31525, CVE-2021-29923, CVE-2021-27918, CVE-2020-16845, CVE-2020-15586, CVE-2021-33195, CVE-2020-28362, CVE-2020-14039, CVE-2021-3114, CVE-2021-3737, CVE-2021-3426, CVE-2021-4189, CVE-2021-42248, CVE-2022-27191, CVE-2022-36313, CVE-2022-45061, CVE-2020-10735, CVE-2022-0391)
Description	IBM has released security updates addressing the multiple vulnerabilities in their products. Exploitation of these vulnerabilities may lead to Arbitrary file creation/overwrite, Path traversal, Buffer overflow, Privilege escalation. IBM recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	IBM Cloud Pak for Security 1.10.0.0 - 1.10.11.0 QRadar Suite Software 1.10.12.0 - 1.10.16.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7080058

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31085, CVE-2023-45871, CVE-2023-25775, CVE-2023-5345, CVE-2023-5090, CVE-2023-5633, CVE-2023-4244)
Description	Ubuntu has released security updates addressing the multiple vulnerabilities that exists in their products. These vulnerabilities may allow an attacker to cause Denial of Service and Arbitrary code execution. Ubuntu recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Ubuntu 18.04 Ubuntu 20.04 Ubuntu 22.04 Ubuntu 23.04 Ubuntu 23.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6495-1 https://ubuntu.com/security/notices/USN-6502-1 https://ubuntu.com/security/notices/USN-6503-1

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.