Advisory Alert

Alert Number: AAA20231206 **Date:** December 6, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple active debug code security vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Solarwinds	**Medium**	HTML Injection Vulnerability

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple active debug code security vulnerabilities(CVE-2023-44297, CVE-2023-44298)
Description	Dell has released security updates addressing multiple active debug code security vulnerabilities in Dell PowerEdge platforms 16G Intel E5 BIOS and Dell Precision BIOS version 1.4.4. An unauthenticated physical attacker could potentially exploit this vulnerability, leading to information disclosure, information tampering, code execution, denial of service. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Precision 7960 Rack BIOS Version 1.4.4 Precision 7960 XL Rack BIOS Version 1.4.4 PowerEdge R660 BIOS Version 1.4.4 PowerEdge R760 BIOS Version 1.4.4 PowerEdge C6620 BIOS Version 1.4.4 PowerEdge MX760c BIOS Version 1.4.4 PowerEdge R860 BIOS Version 1.4.4 PowerEdge R960 BIOS Version 1.4.4 PowerEdge HS5610 BIOS Version 1.4.4 PowerEdge HS5620 BIOS Version 1.4.4 PowerEdge R660xs BIOS Version 1.4.4 PowerEdge R760xs BIOS Version 1.4.4 PowerEdge R760xd2 BIOS Version 1.4.4 PowerEdge T560 BIOS Version 1.4.4 PowerEdge R760xa BIOS Version 1.4.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000218135/dsa-2023-374 https://www.dell.com/support/kbdoc/en-us/000220047/dsa-2023-429-security-update-for-dell-16g-poweredge-server-bios-for-a-debug-code-security-vulnerability

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44487, CVE-2023-20275)
Description	Cisco has released a security update addressing Denial of service and VPN Packet Validation vulnerabilities that exist in their products. **CVE-2023-44487** - HTTP/2 protocol-level weakness in multiple cisco products which enables a novel distributed “Rapid Reset” denial of service (DDoS) attack **CVE-2023-20275**- A vulnerability in the AnyConnect SSL VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to send packets with another VPN user's source IP address. Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple Cisco products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssl-vpn-Y88QOm77 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http2-reset-d8Kf32vZ#vp

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44270, CVE-2023-45133)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in QRadar User Behavior Analytics. Successful exploitation of these vulnerabilities could lead to security bypass and arbitrary code execution. **CVE-2023-44270**- Vulnerability in PostCSS could allow a remote attacker to bypass security restrictions, caused by improper input validaiton. By using a specially crafted external Cascading Style Sheets (CSS), an attacker could exploit this vulnerability to cause \r discrepancies in linters. **CVE-2023-45133-** Babel could allow a local attacker to execute arbitrary code on the system, caused by a flaw in the path.evaluate()or path.evaluateTruthy(). By using a specially crafted code to compile, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	QRadar User Behavior Analytics versions 1.0.0 - 4.1.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7090362

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5158, CVE-2023-39194, CVE-2023-39193, CVE-2023-5178, CVE-2023-39198, CVE-2023-6039, CVE-2023-39192, CVE-2023-3773, CVE-2023-37453, CVE-2023-5717, CVE-2023-39189, CVE-2023-42754, CVE-2023-46862, CVE-2023-46813, CVE-2023-45871, CVE-2023-20593, CVE-2023-45862, CVE-2023-31085.)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to denial of service , out-of-bounds read, sensitive information disclosure, arbitrary code execution Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 23.04 Ubuntu 22.04 LTS Ubuntu 16.04 ESM Ubuntu 14.04 ESM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6534-1 https://ubuntu.com/security/notices/USN-6533-1 https://ubuntu.com/security/notices/USN-6532-1

Affected Product	**Solarwinds**
Severity	**Medium**
Affected Vulnerability	HTML Injection Vulnerability (CVE-2023-40053)
Description	Solarwinds has released a security update addressing a HTML Injection Vulnerability within Serv-U 15.4 that allows an authenticated actor to insert content on the file share function feature of Serv-U, which could be used maliciously. Solarwinds recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Solarwinds Serv-U 15.4 HF2 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2023-40053

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.