Advisory Alert

Alert Number: AAA20230119 **Date:** January 19, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Arbitrary code execution vulnerability
Cisco	**High, Medium**	Multiple vulnerabilities
Ubuntu	**Medium**	Multiple vulnerabilities
Drupal	**Medium**	Multiple vulnerabilities

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Arbitrary code execution vulnerability (CVE-2022-34398)
Description	Dell has released a security update addressing an Arbitrary code execution vulnerability in their products. **CVE-2022-34398-** The vulnerability exists due Time-of-check Time-of-use vulnerability in Dell BIOS. Local authenticated malicious user may potentially exploit this vulnerability by using a specifically timed DMA transaction during an SMI to gain arbitrary code execution on the system. Dell recommends to apply the necessary fixes at your earliest to avoid issues.
Affected Products	Dell Latitude 13 3380, 3120, 3180, 3189, 3190, 3190 2-in-1, 3300, 3310, 3310 2-in-1, 3390 2-in-1, 3490, 3590, 5280, 5285 2-in-1, 5288, 5289, 5290, 5290 2-in-1, 5300, 5300 2-in-1, 5310, 5310 2-in-1, 5400, 5401, 5410, 5411, 5414 Rugged, 5420 Rugged, 5424 Rugged, 5480, 5488, 5490, 5491, 5500, 5501, 5510, 5511, 5580, 5590, 5591, 7200 2-in-1, 7210 2-in-1, 7212 Rugged Extreme Tablet, 7214 Rugged Extreme, 7220 Rugged Extreme Tablet, 7220EX Rugged Extreme Tablet, 7275 2-in-1, 7280, 7285 2-in-1, 7290, 7300, 7310, 7370, 7380, 7389, 7390, 7390 2-in-1, 7400, 7400 2-in-1, 7410, 7414 Rugged Extreme, 7424 Rugged Extreme, 7480, 7490, 9410, 9510, E7270, E7470, Dell OptiPlex 3050, 3050 All-In-One, 3060, 3070, 3080, 3090, 3280 All-In-One, 5050, 5060, 5070, 5080, 5250, 5260 All-In-One, 5270 All-In-One, 5480 All-In-One, 7050, 7060, 7070, 7070 Ultra, 7071, 7080, 7450, 7460 All-In-One, 7470 All-In-One, 7480 All-In-One, 7760 All-In-One, 7770 All-In-One, 7780 All-In-One, XE3 Dell Precision 3240 Compact,3420 Tower, 3430 Tower, 3431 Tower, 3440, 3510, 3520, 3530, 3540, 3541, 3550, 3551, 3620 Tower, 3630 Tower, 3640 Tower,3930 Rack, 5520, 5530, 5530 2-in-1,5540, 5720 All-In-One, 5820 Tower, 7510, 7520, 7530, 7540, 7550, 7710, 7720, 7730, 7740, 7750, 7820 Tower, 7920 Tower Dell Vostro 3070, 3267, 3268, 3470, 3471, 3480, 3481, 3580, 3581, 3582, 3583, 3584, 3667, 3668, 3669, 3670, 3671, 3681, 3881, 3888, 5090, 5880, 7590 Dell Inspiron 3280,3470,3471,3480,3481,3482, 3502, 3510, 3521, 3580, 3583, 3581, 3582,3584, 3670, 3671, 3780, 3781,3782,3880,3881, 5400, 5401 All-In-One, 5477, 5480, 5481 2-in-1, 5490 All-In-One, 5570, 5680, 5770, 7590, 7591, 7700 All-In-One, 7777, 7790, 5491 All-In-One Wyse 5070 Wyse 5470,5470 All-In-One Wyse 7040 Thin Client XPS 15 9575 2-in-1, 7590 XPS 8930, 8940, 895 Aurora R14 ChengMing 3980,3988, 3990, 3991 Dell G3 15 3590, 3579, 3779 Dell G5 15 5590, 5000, 5090 Dell G7 15 7590, 17 7790 Dell Latitude 3480, 3580 Edge Gateway 3000 series, 5000 Embedded Box PC 3000, PC 5000
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000206038/dsa-2022-339-dell-client-security-update-for-a-dell-client-bios-vulnerability

Affected Product	**Cisco**
Severity	**High, Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-20010, CVE-2023-20057)
Description	Cisco has released a security update addressing Multiple vulnerabilities in their products. If exploited, these vulnerabilities can lead to URL Filtering Bypass and SQL Injection. **CVE-2023-20010-** This vulnerability exists because the web-based management interface inadequately validates user input. An attacker could exploit this vulnerability by authenticating to the application as a low-privileged user and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to read or modify any data on the underlying database or elevate their privileges. **CVE-2023-20057-** This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco Unified CM, Unified CM SME Release 12.5(1)c and Release 14 All releases of Cisco AsyncOS Software for Cisco ESA.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-sql-rpPczR8n https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-22809, CVE-2022-33070)
Description	Ubuntu has released a security update addressing Multiple vulnerabilities in their products. If exploited, these vulnerabilities can lead to Arbitrary code execution and Denial of Service. **CVE-2023-22809-** This vulnerability exists due to incorrectly handled user-specified editors when using the sudoedit command. A local attacker that has permission to use the sudoedit command could possibly use this to edit arbitrary files. **CVE-2023-33070-** This vulnerability exists in the Protobuf-c library, used by Sudo, incorrectly handled certain arithmetic shifts. An attacker could possibly use this issue to cause Sudo to crash, resulting in a denial of service. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 16.04 Ubuntu 18.04 Ubuntu 20.04 Ubuntu 22.04 Ubuntu 22.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5811-1 https://ubuntu.com/security/notices/USN-5811-2

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability
Description	Drupal has released a security update addressing Information Disclosure Vulnerability in their Drupal Core, Drupal Entity browser, Drupal Media Library Block module and Form API Element. Drupal recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Drupal 8.0.0 <9.4.10 Drupal 9.5.0 <9.5.2 Drupal 10.0.0 -10.0.2 Drupal Entity Browser before 8.x-2.9. Drupal Media Library Block module 1.0 <1.0.4 Drupal Media Library Form API Element 2.0 <2.0.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2023-001 https://www.drupal.org/sa-contrib-2023-002 https://www.drupal.org/sa-contrib-2023-003 https://www.drupal.org/sa-contrib-2023-004

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.