Advisory Alert

Alert Number: AAA20230202 **Date:** February 2, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Time-of-check Time-of-use vulnerability
HP	**High**	Use After Free Vulnerability
Cisco	**High**, Medium	Multiple Vulnerabilities
Drupal	Medium	Access Bypass Vulnerability
IBM	Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Dell**	
Severity	**High**	
Affected Vulnerability	Time-of-check Time-of-use vulnerability (CVE-2022-34398)	
Description	Dell has released a security updates to address a Time-of-check Time-of-use vulnerability that exist in the Dell BIOS. Using this vulnerability a local authenticated attacker can execute arbitrary code on the system by using a specifically timed DMA transaction during an SMI. Dell recommends to apply necessary security fixes at earliest to avoid issues	
Affected Products	Alienware Area 51m R1 Alienware Area 51m R2 Alienware Aurora R10 Alienware Aurora R11 Alienware Aurora R12 Alienware Aurora R13 Alienware Aurora R8 Alienware Aurora R9 Alienware m15 R1 Alienware m15 R2 Alienware m15 R3 Alienware m15 R4 Alienware m17 R1 Alienware m17 R2 Alienware m17 R3 Alienware m17 R4 Alienware x14 Alienware x15 R1 Alienware x15 R2 Alienware x17 R1 Alienware x17 R2 Aurora R14 ChengMing 3980 ChengMing 3988 ChengMing 3990 ChengMing 3991 Dell G3 15 3590 Dell G3 3579 Dell G3 3779 Dell G5 15 5590 Dell G5 5000	Dell G5 5090 Dell G7 15 7590 Dell G7 17 7790 Dell Latitude 3480 Dell Latitude 3580 Edge Gateway 3000 series Edge Gateway 5000 Embedded Box PC 3000 Embedded Box PC 5000 Inspiron 3280 Inspiron 3470 Inspiron 3471 Inspiron 3480 Inspiron 3481 Inspiron 3482 Inspiron 3502 Inspiron 3510 Inspiron 3521 Inspiron 3580 Inspiron 3583 Inspiron 3581 Inspiron 3584 Inspiron 3582 Inspiron 3670 Inspiron 3671 Inspiron 3780 Inspiron 3781 Inspiron 3782 Inspiron 3880 Inspiron 3881
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	**HP**
Severity	**High**
Affected Vulnerability	Use After Free Vulnerability (CVE-2022-40674)
Description	HP has released a security update addressing a vulnerability that exists in HPE OneView. **CVE-2022-40674** – Due to a vulnerability that exist in the expat open source library it is possible to create a situation in which parsing is suspended while substituting in an internal entity so that XML_ResumeParser directly uses the internalEntityProcessor as its processor. If the subsequent parse includes some unclosed tags, this will return without calling storeRawNames to ensure that the raw versions of the tag names are stored in memory other than the parse buffer itself. Issues occur if the parse buffer is changed or reallocated, problems occur. Using this vulnerability an attacker can execute arbitrary code in the system and perform denial of service attacks. HP recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	HPE OneView Prior to 8.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04402en_us

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20076, CVE-2023-20073, CVE-2023-20030, CVE-2023-20021, CVE-2023-20022, CVE-2023-20023, CVE-2023-20068)
Description	Cisco has released Security Updates addressing Multiple Vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could cause arbitrary command execution, arbitrary file upload, sensitive information disclosure, command injection and conduct reflected cross site scripting (XSS). Cisco recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Cisco 800 Series Industrial ISRs Cisco Catalyst Access Points (COS-APs) Cisco CGR1000 Compute Modules Cisco IC3000 Industrial Compute Gateways software releases earlier than 1.2.1 Cisco IOS XE-based devices configured with IOx Cisco IR510 WPAN Industrial Routers Cisco RV340 Dual WAN Gigabit VPN Routers Cisco RV340W Dual WAN Gigabit Wireless-AC VPN Routers Cisco RV345 Dual WAN Gigabit VPN Routers Cisco RV345P Dual WAN Gigabit POE VPN Router Cisco ISE Software Release version 3.2 and earlier versions Cisco Prime Infrastructure Release Earlier than 3.10.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-afu-EXxwA65V https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-GecEHY58 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-os-injection-pxhKsDM https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pi-xss-PU6dnfD9

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Access Bypass Vulnerability
Description	Drupal has released a Security Update addressing an access bypass vulnerability that exist in Apigee Edge product. This vulnerability exists due to the Apigee Edge module allows connecting a Drupal site to Apigee X / Edge in order to build a developer portal. Drupal recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Apigee Edge module version 2.0.x for Drupal 9.x Apigee Edge module version 8.x-1.x for Drupal 9.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2023-005

Affected Product	**IBM**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-21628, CVE-2022-21626, CVE-2022-21624, CVE-2022-21619, CVE-2022-3676)
Description	IBM has released a Security Update addressing multiple vulnerabilities that effects the IBM WebSphere Application Server **CVE-2022-21628** – A denial of service vulnerability that exist in the Java SE that caused by the flaw in the Lightweight HTTP Server. A remote attacker could exploit this vulnerability by sending an specially-crafted request. **CVE-2022-21626 –** An unspecified vulnerability that exist in the Java SE related to the Security component. An unauthenticated attacker can exploit this vulnerability to cause denial of service. **CVE-2022-21624 –** An unspecified vulnerability that exist in the Java SE related to the Security component. An unauthenticated attacker can exploit this vulnerability to update, insert or delete data resulting in a low integrity impact using unknown attack vectors **CVE-2022-21619** - An unspecified vulnerability that exist in the Java SE related to the Security component. An unauthenticated attacker can exploit this vulnerability to update, insert or delete data resulting in a low integrity impact using unknown attack vectors. **CVE-2022-3676** – Eclipse Openj9 could allow a remote attacker to bypass security restrictions, caused by improper runtime type check by the interface calls. By sending a specially-crafted request using bytecode, an attacker could exploit this vulnerability to access or modify memory. IBM recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	IBM Java SDK shipped with IBM WebSphere Application Server Patterns 1.0.0.0 through 1.0.0.7 and 2.2.0.0 through 2.3.3.5.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6912697

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.