Advisory Alert

Alert Number: AAA20231019 **Date:** October 19, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
CPanel	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Cisco	**Medium**	Local File Inclusion Vulnerability
HPE	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-21930, CVE-2023-21967, CVE-2023-21954, CVE-2023-21939, CVE-2023-21968, CVE-2023-21937, CVE-2023-21938, CVE-2023-2597, CVE-2023-31484, CVE-2023-31486)
Description	IBM has released security updates addressing multiple vulnerabilities that affect their products. Exploitation of these vulnerabilities could lead to Man-In-The-Middle attack, unauthorized update, insert or delete access. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Db2 10.5.0.x Client and Server IBM Db2 11.1.4.x Client and Server IBM Db2 11.5.x Client and Server AIX 7.2 AIX 7.3 VIOS 3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7047272 https://www.ibm.com/support/pages/node/7047556

Affected Product	**CPanel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45143, CVE-2023-44487, CVE-2023-39331, CVE-2023-39332, CVE-2023-39333, CVE-2023-38552)
Description	CPanel has released a security update addressing multiple vulnerabilities that affect their products. Exploitation of these vulnerabilities could lead to Path traversal, Denial of Service, Cookie leakage, Verification bypass. CPanel recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	cPanel packages for EasyApache 4 with NodeJS versions 18.18.2 and 20.8.1.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2023-10-18-maintenance-and-security-release/

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Local File Inclusion Vulnerability (CVE-2023-20261)
Description	Cisco has released a security update addressing a Local File Inclusion vulnerability that exist in web UI of Cisco Catalyst SD-WAN Manager. Successful exploitation could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. Cisco recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	web UI of Cisco Catalyst SD-WAN Manager Earlier than 20.6.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-30911)
Description	HPE has released a security update addressing a Denial of Service vulnerability that exist in HPE Integrated Lights-Out products. HPE recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us

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.