Advisory Alert

Alert Number: **AAA20231117** **Date:** **November 17, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Multiple Vulnerabilities
Cisco	**High**	Denial of Service Vulnerability
cPanel	Low	Security Update

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-23583)
Description	HPE has released security updates addressing multiple vulnerabilities exists in their products. Successful exploitation of these vulnerabilities could lead to privilege escalation lead denial of service and information disclosure. HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HPE ProLiant DX220n Gen10 Plus server - Prior to 1.90_10-19-2023 HPE ProLiant DX360 Gen10 Plus server - Prior to 1.90_10-19-2023 HPE ProLiant DX380 Gen10 Plus server - Prior to 1.90_10-19-2023 HPE Apollo 2000 Gen10 Plus System - Prior to 1.90_10-19-2023 HPE Apollo 4200 Gen10 Plus System - Prior to 1.90_10-19-2023 HPE ProLiant XL220n Gen10 Plus Server - Prior to 1.90_10-19-2023 HPE ProLiant XL290n Gen10 Plus Server - Prior to 1.90_10-19-2023
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04556en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04557en_us

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-20083)
Description	Cisco has released security update addressing Denial of Service Vulnerability exists in their products. **CVE-2023-20083** - Denial of Service vulnerability due to improper error checking when parsing fields within the ICMPv6 header. An attacker could exploit this vulnerability by sending a crafted ICMPv6 packet through an affected device. A successful exploit could allow the attacker to cause the device to exhaust CPU resources and stop processing traffic, resulting in a DoS condition. Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco products configured with a network discovery policy that enables both host and application detection and invokes the Snort 2 Detection Engine FirePOWER Services - All platforms Firepower Threat Defense (FTD) Software - All platforms
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-icmpv6-dos-4eMkLuN

Affected Product	**cPanel**
Severity	Low
Affected Vulnerability	Security Update
Description	cPanel has released a security update addressing a encoding issue in cPanel access_log. When incoming requests to cpsrvd that contained control and other non-printable characters arrived, characters got logged without being properly encoded. In this security release, cPanel ensures that these characters are properly ASCII encoded before being logged. cPanel recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	cPanel Builds before 11.116.0.4 cPanel Builds before 11.114.0.12 cPanel Builds before 11.110.0.15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/cpanel-tsr-2023-0004-full-disclosure/

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.