



Advisory Alert

Alert Number: AAA20230309

Date: March 9, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	High , Medium	Multiple Vulnerabilities
HPE	Medium	Multiple Vulnerabilities

Description

Affected Product	Cisco
Severity	High , Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20064, CVE-2023-20049)
Description	<p>Cisco has released security updates addressing multiple vulnerabilities. Exploitation of these vulnerabilities can lead to Information Disclosure, Denial of Service Vulnerability.</p> <p>CVE-2023-20064 - An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device.</p> <p>CVE-2023-20049 - An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads.</p> <p>Cisco recommends to apply necessary security fixes at earliest to avoid issues</p>
Affected Products	ASR 9000 Series Aggregation Services Routers (64-bit) IOS XR White box IOS XRv 9000 Routers Network Convergence System (NCS) 540 Series Routers NCS 560 Series Routers NCS 1001 Series Routers NCS 1002 Series Routers NCS 1004 Series Routers NCS 5000 Series Routers NCS 5500 Series Routers NCS 5700 Series Routers NCS 6000 Series Routers ASR 9000 Series Aggregation Services Routers only if they have a Lightspeed or Lightspeed-Plus-based line card installed ASR 9902 Compact High-Performance Routers ASR 9903 Compact High-Performance Routers
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq

Affected Product	HPE
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-37940)
Description	<p>HPE has released security updates addressing multiple vulnerabilities that exist in HPE FlexFabric 5700 Switch Series. A remote attacker can exploit this vulnerabilities to allow host header injection and URL redirection.</p> <p>HPE recommends to apply the patch updates at earliest to avoid issues</p>
Affected Products	HPE FlexFabric 5700 Switch Series - Prior to R2432P61
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04398en_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.