Advisory Alert

Alert Number: AAA20220915 **Date:** September 15, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Medium**	Denial-of-service Vulnerability
Paloalto	**Medium**	Improper Link Resolution Vulnerability

Description

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Denial-of-service vulnerability (CVE-2022-20845, CVE-2022-20846, CVE-2022-20849)
Description	Cisco has released Security Updates addressing multiple vulnerabilities in their products. **CVE-2022-20845** - A vulnerability exist in the TL1 function of Cisco Network Convergence System due to TL1 not freeing memory. An attacker could cause the TL1 process to consume large amounts of memory. When the memory reaches a threshold, the Resource Monitor process will begin to restart or shutdown the top five consumers of memory, resulting in a denial of service. **CVE-2022-20846** - A vulnerability exist in the Cisco Discovery Protocol implementation for Cisco IOS XR Software due to heap buffer overflow in certain Cisco Discovery Protocol messages. An attacker could cause a heap overflow by sending malicious Cisco Discovery Protocol packet. The bytes that can be written in the buffer overflow are restricted, which limits remote code execution. **CVE-2022-20849** - A vulnerability exist in the Broadband Network Gateway PPP over Ethernet feature of Cisco IOS XR Software due PPPoE feature does not properly handle an error condition within a specific crafted packet sequence. An attacker could cause a PPPoE process to continually restart by sending a sequence of specific PPPoE packets resulting in a denial of service condition. Cisco recommends to apply relevant patches at earliest to avoid issues.
Affected Products	Cisco NCS 4000 Series running Cisco IOS XR Earlier than 6.5.32 Cisco IOS XR Software 5.2.2 and later had the Cisco Discovery Protocol feature enabled ASR 9000 Series Aggregation Services Routers Cisco IOS XR Software 5.2.2 and later had the Broadband Network Gateway PPPoE enabled, running Cisco IOS XR v6.8 and earlier, v7.1- 7.4, v7.5 IOS XRv 9000 Routers Cisco IOS XR Software had the Broadband Network Gateway PPPoE enabled, running Cisco IOS XR v6.8 and earlier, v7.1- 7.4, v7.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ncs4k-tl1-GNnLwC6 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xr-cdp-wnALzvT2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-bng-Gmg5Gxt

Affected Product	**Paloalto**
Severity	**Medium**
Affected Vulnerability	Improper Link Resolution Vulnerability (CVE-2022-0029)
Description	Paloalto has released a Security Update addressing an Improper Link Resolution Vulnerability in the Cortex XDR Agent on windows devices. Successful exploit could allow the attacker to read files on the system with elevated privileges when generating a tech support file. Paloalto recommends to apply relevant patches at earliest to avoid issues.
Affected Products	Cortex XDR Agent 7.5 CE < 7.5.101-CE on Windows Cortex XDR Agent 7.7 < 7.7.3 on Windows Cortex XDR Agent 5.0 < 5.0.12-hotfix update on Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2022-0029

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.