Advisory Alert

Alert Number: AAA20220825 **Date:** August 25, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**Cisco**	
Severity	**High**, **Medium**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20865, CVE-2022-20921, CVE-2022-20823, CVE-2022-20824)	
Description	Cisco has released Security Updates addressing multiple vulnerabilities in their products. **CVE-2022-20865** - A vulnerability exist in the CLI of Cisco FXOS Software due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command leading to command execution on the underlying operating system with root privileges. **CVE-2022-20921 -** A vulnerability exists in the API implementation of Cisco ACI Multi-Site Orchestrator (MSO) due to improper authorization on specific APIs. An attacker could exploit this vulnerability by sending crafted HTTP requests. A successful exploit could allow an attacker who is authenticated with non-Administrator privileges to elevate to Administrator privileges on an affected device. **CVE-2022-20823 -** A vulnerability exists in the OSPF version 3 (OSPFv3) feature of Cisco NX-OS Software due to incomplete input validation of specific OSPFv3 packets. An attacker could exploit this vulnerability by sending a malicious OSPFv3 link-state advertisement (LSA) to an affected device. A successful exploit could allow the attacker to cause the OSPFv3 process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition. **CVE-2022-20824 -** A vulnerability exists in the Cisco Discovery Protocol feature of Cisco FXOS Software and Cisco NX-OS Software due to improper input validation of specific values that are within a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges or cause the Cisco Discovery Protocol process to crash and restart multiple times, which would cause the affected device to reload, resulting in a DoS condition. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.	
Affected Products	Firepower 4100 Series Firepower 9300 Security Appliances Cisco ACI MSO Release 3.0 and earlier Cisco ACI MSO Release 3.1 Firepower 9300 Security Appliances MDS 9000 Series Multilayer Switches Nexus 1000 Virtual Edge for VMware vSphere Nexus 1000V Switch for Microsoft Hyper-V Nexus 1000V Switch for VMware vSphere Nexus 3000 Series Switches	Nexus 5500 Platform Switches Nexus 5600 Platform Switches Nexus 6000 Series Switches Nexus 7000 Series Switches Nexus 9000 Series Fabric Switches in ACI mode Nexus 9000 Series Switches in standalone NX-OS mode UCS 6200 Series Fabric Interconnects UCS 6300 Series Fabric Interconnects UCS 6400 Series Fabric Interconnects Nexus 9000 Series Fabric Switches in ACI mode
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-cmdinj-TxcLNZNH https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mso-prvesc-BPFp9cZs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cdp-dos-ce-wWvPucC9 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ospfv3-dos-48qutcu	

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.