Advisory Alert

Alert Number: AAA20220303 **Date:** March 3, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20754, CVE-2022-20755, CVE-2022-20756, CVE-2022-20665)
Description	Cisco has released Security Updates addressing multiple vulnerabilities that exist with various cisco products such as Arbitrary File Write Vulnerability, Command Injection Vulnerability, and Denial of Service Vulnerability. It is highly recommended to apply necessary fixes provided on the official Cisco website at the earliest to avoid these security issues, and all Cisco users are encouraged to upgrade to the latest versions.
Affected Products	Cisco Expressway Series Cisco TelePresence VCS Cisco ISE ASR 5000 Series Routers Ultra Cloud Core - User Plane Function Virtualized Packet Core - Distributed Instance (VPC-DI) Virtualized Packet Core - Single Instance (VPC-SI)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-filewrite-87Q5YRk https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-dos-JLh9TxBp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-staros-cmdinj-759mNT4n

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.