Advisory Alert

Alert Number : AAA20210401 **Date :** April 1, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	**Fast Reload Vulnerabilities**

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Fast Reload Vulnerabilities (CVE-2021-1375, CVE-2021-1376)
Description	The vulnerability exists in the fast reload feature of Cisco IOS XE Software running on Cisco Series Switches due to incorrect validation of parameters passing to configuration file for executed when the device boots up with a malicious software image. A successful exploit could allow the attacker to either execute arbitrary code on the operating system or execute unsigned code and bypass the image verification check part of the secure boot process.
Affected Products	Cisco Catalyst 3650, Cisco Catalyst 3850, Cisco Catalyst 9300, and Cisco Catalyst 9300L Series Switches
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fast-Zqr6DD5

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.