Advisory Alert

Alert Number: AAA20210709 **Date:** July 9, 2021

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	**Denial of Service**

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Denial of Service (CVE-2018-0155)
Description	Cisco has released security updates addressing Denial of Service that exists in their products. A remote attacker can send a specially crafted Bidirectional Forwarding Detection (BFD) packet to or through the target device to trigger an error handling flaw and cause the target 'iosd' process to crash and the system to reload. Cisco recommends to apply necessary security fixes to avoid issues.
Affected Products	The following models are affected when the BFD feature is enabled Catalyst 4500 Supervisor Engine 6-E (K5) Catalyst 4500 Supervisor Engine 6L-E (K10) Catalyst 4500 Supervisor Engine 7-E (K10) Catalyst 4500 Supervisor Engine 7L-E (K10) Catalyst 4500E Supervisor Engine 8-E (K10) Catalyst 4500E Supervisor Engine 8L-E (K10) Catalyst 4500E Supervisor Engine 9-E (K10) Catalyst 4500-X Series Switches (K10) Catalyst 4900M Switch (K5) Catalyst 4948E Ethernet Switch (K5)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-bfd

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.