Advisory Alert

Alert Number: AAA20220819 **Date:** August 19, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Privilege Escalation Vulnerability

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2022-20871)
Description	Cisco has released a security update addressing the Privilege Escalation Vulnerability in the web management interface of Cisco AsyncOS for Cisco Secure Web Appliance. This vulnerability could allow the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root. It's due to insufficient validation of user-supplied input for the web interface. To successfully exploit this vulnerability, an attacker would need at least read-only credentials. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco AsyncOS for Secure Web Appliance Release 12.5 Cisco AsyncOS for Secure Web Appliance Release 14.0 Cisco AsyncOS for Secure Web Appliance Release 14.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-prv-esc-8PdRU8t8

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.