Advisory Alert

Alert Number: AAA20210122 **Date:** January 22, 2021

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
Description	A vulnerability in Cisco Secure Web Appliance could allow an authenticated, local attacker to perform command injection and elevate privileges to root. This occurs due to insufficient validation of user input for the web interface and CLI. An attacker could exploit this vulnerability by authenticating to the device and injecting commands. If an attacker successfully exploit the vulnerability, he can execute arbitrary commands on the underlying operating system and elevate privileges to root.
Affected Products	Cisco AsyncOS for the Secure Web Appliance, (both virtual and hardware appliances.)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-prv-esc-nPzWZrQj

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.