Advisory Alert

Alert Number: AAA20210802 **Date:** **August 2, 2021**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Privilege Escalation
Nodejs	**High**	Buffer Overflow

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Privilege Escalation (CVE-2021-1359)
Description	A vulnerability in the configuration management of Cisco AsyncOS for Cisco Web Security Appliance could allow an authenticated, remote attacker to perform command injection and elevate privileges to root. An attacker could exploit this vulnerability by uploading crafted XML configuration files that contain scripting code to a vulnerable device.
Affected Products	Cisco AsyncOS for Cisco WSA, 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-scr-web-priv-esc-k3HCGJZ

Affected Product	**Nodejs**
Severity	**High**
Affected Vulnerability	Buffer Overflow (CVE-2021-22930)
Description	Node.js is vulnerable to a use after free attack where an attacker might be able to exploit the memory corruption, to change process behavior. **Use-After-Free (UAF)** is a vulnerability related to incorrect use of dynamic memory during program operation
Affected Products	Node v12.22.4 (LTS) Node v14.17.4 (LTS)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/release/v14.17.4/ https://nodejs.org/en/blog/release/v12.22.4/

Disclaimer

Financial Sector Computer Security Incident Response Team (FinCSIRT)
LankaClear Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka
Hotline: + 94 112039777