UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00169

CISCO ASA, BPA & WSA VULNERABILITIES

DATE ISSUED: 12th July 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

High-severity privilege escalation vulnerabilities have been discovered in Cisco's Business Process Automation (BPA) and Web Security Appliance (WSA) that could allow remote access or device takeover if exploited. Attacks against the Cisco Adaptive Security Appliance (ASA) have also been seen in the wild.

BREAKDOWN

CVE-2020-3580 affecting Cisco's ASA have been seen in the wild using Cross Site Scripting (XSS) attacks and a Proof of Concept (PoC) has been dropped on Twitter by Positive Technologies researchers – which they called "low-hanging fruit"

Two other bugs CVE-2021-1574 (execute unauthorised commands) and CVE-2021-1576 (retrieve sensitive data with valid login credentials) exist in the web-based interface of BPA and both have a CVSS rating of 8.8/10 allowing attackers to escalate privileges to administrator levels. Both are due to improper authorisation enforcement. CVE-2021-1359 is rated 6.3/10 is the configuration manager of Cisco AsyncOS responsible for powering WSA allowing an authenticated users to gain root level access. This is a result of insufficient validation of user-supplied XML input allowing the upload of XML files and resulting arbitrary code execution.

REMEDIATION STEPS

- Patch ASA Appliances with updates available from Cisco. Upgrade virtual and hardware-based appliances running 11.8, 12.0 and 12.5.
- Upgrade any instances using BPA running versions prior to 3.1.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/cisco-asa-bug-exploited-poc/167274/
	https://threatpost.com/cisco-bpa-wsa-bugs-cyberattacks/167654/
Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-xss-multiple-FCB3vPZe
	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-scr-web-priv-esc-k3HCGJZ