CyberSOC Threat Notification

Active Exploitation of Fortinet FortiOS Vulnerabilities

Executive Summary

On April 2nd, 2021, the FBI and CISA released a joint Cybersecurity Advisory to warn that Advanced Persistent Threat (APT) actors are actively exploiting known Fortinet FortiOS vulnerabilities.

Description

APT actors are actively exploiting these three known Fortinet FortiOS vulnerabilities to gain access to multiple government, commercial, and technology services. The actors are scanning devices on ports 4443, 8443, and 10443 for CVE-2018-13379, and enumerated devices for CVE-2020-12812 and CVE-2019-5591. These exploits will help the actors gain initial access and pre-position them to conduct future attacks.

Affected Products

- CVE-2020-12812
  - FortiOS 6.4.0, 6.2.0, 6.2.3, 6.0.9 and below
- CVE-2019-5591
  - FortiOS 6.2.0 and below
- CVE-2018-13379
  - FortiOS 6.0.0 to 6.0.4
  - FortiOS 5.6.3 to 5.6.7
  - FortiOS 5.4.6 to 5.4.12

Safeguards/Recommendations

Affected customers are strongly encouraged to review the advisory and immediately update any device running FortiOS to the newest version.

Version History

Version 1. Initial Report

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io

Vendor: Fortinet

CVE-ID: Multiple

CVE-2020-12812,
CVE-2019-5591,
CVE-2018-13379

Published: April 02, 2021

CVSS V3 Overall score: 9.8, 7.5, 9.8

Criticality: Critical, High, Critical

Patch Availability: Yes

Vulnerability Type: Multiple

Improper Authentication,
Man in the Middle,
Path Traversal

Exploitability Metrics

Attack Vector: Remote

Attack Complexity: Low

Privileges Required: None

User Interaction: None

Impact Metrics

Scope: Unchanged

Confidentiality: High

Integrity: High

Availability: High

Confidence Metrics

Exploitability: Not Defined

Remediation Level: Not Defined

Report Confidence: Not Defined