Cisco security appliance 0-day is under attack by ransomware crooks

Enlarge / Cisco Systems headquarters in San Jose, California, US, on Monday, Aug. 14, 2023. Cisco Systems Inc. is scheduled to release earnings figures on August 16. Photographer: David Paul Morris/Bloomberg via Getty Images

reader comments

9 with

Cisco on Thursday confirmed the existence of a currently unpatched zero-day vulnerability that hackers are exploiting to gain unauthorized access to two widely used security appliances it sells.

The vulnerability resides in Cisco's Adaptive Security Appliance Software and its Firepower Threat Defense, which are typically abbreviated as ASA and FTD. Cisco and researchers have known since last week that a ransomware crime syndicate called Akira was gaining access to devices through password spraying and brute-forcing. Password spraying, also known as credential stuffing, involves trying a handful of commonly used passwords for a large number of usernames in an attempt to prevent detection and subsequent lockouts. In brute-force attacks, hackers use a much larger corpus of password guesses against a more limited number of usernames.

Ongoing attacks since (at least) March

“An attacker could exploit this vulnerability by specifying a default connection profile/tunnel group while conducting a brute force attack or while establishing a clientless SSL VPN session using valid credentials,” Cisco officials wrote in an advisory. “A successful exploit could allow the attacker to achieve one or both of the following:

- *Identify valid credentials that could then be used to establish an unauthorized remote access VPN session.*
- *Establish a clientless SSL VPN session (only when running Cisco ASA Software Release 9.16 or earlier).*

The ASA is an all-in-one security device that provides firewall, antivirus, intrusion prevention, and virtual private network protections. The FTD is Cisco’s next-generation device that combines the ASA capabilities with a finer-grained management console and other more advanced features. The vulnerability, tracked as CVE-2023-20269, stems from the devices’ improper separation of authentication, authorization, and accounting in remote access among their VPN, HTTPS management, and site-to-site VPN features. It has a severity rating of 5.0 out of a possible 10.

Advertisement

Researchers from security firm Rapid7 reported last week that they had observed credential-stuffing and brute-force attacks against ASA devices since at least last March. The attacks were coming from Akira and targeted devices that didn’t have multi-factor authentication enforced for some or all of its users, the researchers said.

“Rapid7 identified at least 11 customers who experienced Cisco ASA-related intrusions between March 30 and August 24, 2023,”

the August 29 post, headlined “Under Siege: Rapid7-Observed Exploitation of Cisco ASA SSL VPNs,” stated. “Our team traced the malicious activity back to an ASA appliance servicing SSL VPNs for remote users. ASA appliance patches varied across compromised appliances—Rapid7 did not identify any particular version that was unusually susceptible to exploitation.”

The attacks, as illustrated in an image included in the Rapid7 post, often directed multiple login attempts at a target in rapid succession. While both login attempts captured in the pictured activity log were unsuccessful, attackers in some cases “successfully authenticated on the first try, which may indicate that the victim accounts were using weak or default credentials.”

https://arstechnica.com/?p=1966724