Akira Ransomware Exploits Cisco ASA/FTD Vulnerability

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued a high-severity warning for a vulnerability in the web services interface of Cisco ASA (Adaptive Security Appliance) and FTD (Firepower Threat Defense) software. The vulnerability, documented as CVE-2020-3259 with a CVSS score of 7.5, can be abused by ransomware campaigns to gain unauthenticated access and gather sensitive information, including usernames and passwords, from the memory of vulnerable Cisco devices. The flaw has been reported to be exploited by Akira ransomware on multiple devices since March 2023, and is at risk from other ransomware campaigns. Attacks from threat actors have involved the use of brute force and password spraying methods to obtain access via VPN software without Multi-factor Authentication (MFA) enabled.

Services at risk are Cisco ASA and FTD software with Cisco AnyConnect IKEv2 Remote Access (with client services) or AnyConnect SSL VPN enabled, and Cisco ASA software with Clientless SSL VPN enabled. Cisco ASA and FTD configurations can be validated via the Cisco Software Checker tool or by entering ‘show-running-config' in the command-line interface (CLI) and reviewing whether the configurations ‘crypto ikev2’ or ‘webvpn’ are enabled. Cisco has since released free software updates to resolve this vulnerability.

CISA has ordered federal agencies to resolve the vulnerability CVE-2020-3259, or discontinue product use if mitigations are unavailable, by March 7, 2024. While CVE-2020-3259 may not be a brand-new threat, it serves as a stark reminder that cybercriminals relentlessly exploit known vulnerabilities to infiltrate organizations. This incident underscores the critical need for robust vulnerability management practices.
