Cisco ASA Cross Site Scripting Vulnerability Exploited in the Wild

Overview

Cisco has updated an old advisory for CVE-2014-2120, a medium-severity cross-site scripting (XSS) vulnerability affecting the WebVPN login page of Cisco Adaptive Security Appliance (ASA) software.

This vulnerability, initially disclosed in 2014, has been exploited in the wild as of November 2024. Threat actors are leveraging this flaw for various malicious activities, including persistence and backdooring.

CVE-2014-2120 (CVSS 4.3) results from insufficient input validation on the WebVPN login page, allowing unauthenticated, remote attackers to conduct XSS attacks. Attackers can exploit the flaw by convincing users to click on a malicious link. Once exploited, attackers can perform unauthorized file uploads, insert malicious code, and compromise sensitive systems.

According to researchers from CloudSEK, the Androxgh0st botnet has been targeting vulnerabilities in various products, including those from Cisco, Atlassian, Metabase, Sophos, Oracle, OptiLink, TP-Link, Netgear, and GPON. It has also exploited weaknesses in PHP and a WordPress plugin, with **one of the flaws being the Cisco ASA vulnerability** (CVE-2014-2120).

Due to the vulnerability being exploited, Aspire recommends that organizations patch as soon as possible.

Aspire Protects

- **Patch –** There are no available workarounds for this vulnerability. Cisco advises customers to contact their usual support channels to upgrade to a fixed software version. However, free software updates are not offered for vulnerabilities disclosed through a Cisco Security Notice.
    - Please see Cisco's advisory for patch guidance.
    - Check the Cisco Bug ID: CSCun19025 for detailed information. Customers will have to input login credentials.
- Enhance network monitoring for signs of unauthorized activity or attempted exploitation, such as crafted WebVPN login page requests.
- Train users to recognize and avoid clicking on suspicious or unexpected links.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application (T1190): Threat actors exploit the WebVPN login page to gain unauthorized access.

Persistence

- Implant Container (T1202): Upload malicious files to maintain control over the compromised system.

Credential Access

- Steal Web Session Cookie (T1539): Utilize XSS to steal sensitive credentials or session information.

Impact

- Network Denial of Service (T1498): Exploit botnet capabilities for distributed denial-of-service (DDoS) attacks.

IoCs

There are no known IoCs associated with CVE-2014-2120 at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The industries impacted by the CVE-2014-2120 vulnerability largely depend on the deployment of Cisco ASA devices, which are commonly used across various sectors for secure network access. The targeted industries may include:

- Government and Public Sector
- Healthcare
- Telecommunications
- Retail and E-commerce
- Education

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
    - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

- Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
- Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cisco Adaptive Security Appliance WebVPN Login Page Cross-Site Scripting Vulnerability

CVE Record | CVE

Mozi Resurfaces as Androxgh0st Botnet: Unraveling The Latest Exploitation Wave | CloudSEK