THREAT BULLETINS

Threat Actors are Exploiting Cisco ASA Software Flaw CVE-2014-2120

TLP:WHITE

Dec 03, 2024

On December 2, 2024, Cisco updated its security advisory concerning a decade-old flaw tracked as CVE-2014-2120 to warn about its exploitation. The flaw exists in the WebVPN login page of Cisco Adaptive Security Appliance (ASA) Software.

The issue affects the WebVPN feature used for secure remote access. The flaw allows threat actors to remotely conduct a cross-site scripting (XSS) attack against a WebVPN user on the vulnerable Cisco ASA device. The flaw was originally disclosed in March 2014, and the company deployed relevant patches.

The exploitation of this old vulnerability highlights the importance of maintaining up-to-date security measures to safeguard against potential threats. No workarounds are available for this flaw. Health-ISAC advises members who use Cisco ASA software to ensure their devices are patched as the only way to mitigate the risk of exploitation.

Recommendations:

- Apply available patches for vulnerable Cisco devices.
- Ensure all of the devices are patched in a timely manner.
- Enforce network segmentation and strict network access control policies.
- Continuously monitor for suspicious activities.

- Have an incident response plan ready to limit operational disruptions in the event of a successful attack.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.

Reference(s)	Security Online, HHS, Cisco

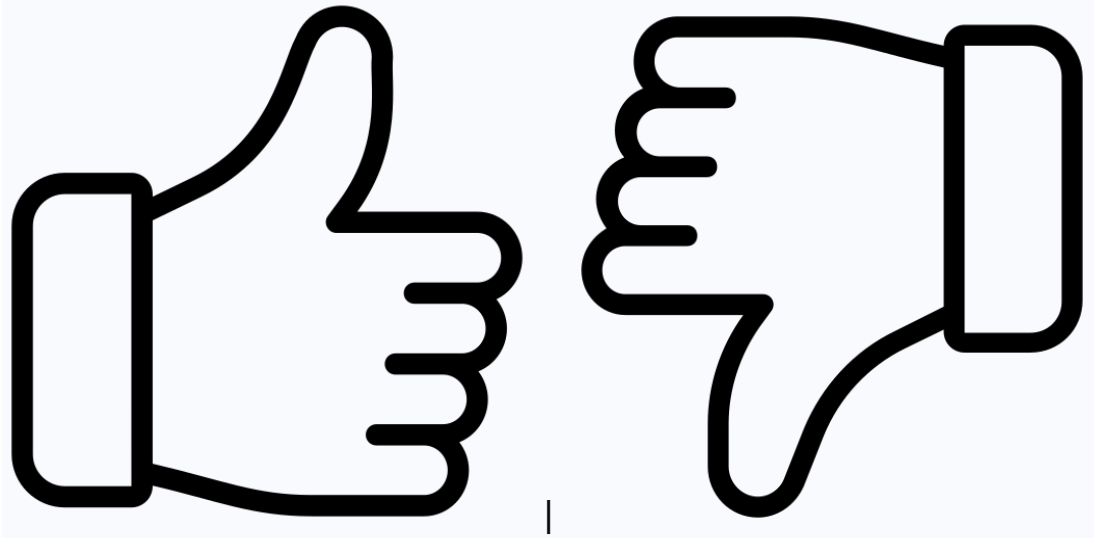
Sources
Cisco Security Advisory
Cisco Confirms Active Exploitation of Decade-Old WebVPN Vulnerability in ASA Software

Incident Date
Dec 03, 2024 (UTC)

Alert ID 94eae089

View Alert

Share Feedback
was this helpful?



Tags CVE-2014-2120, Cisco ASA Software

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Share Threat Intel
For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**