National Cyber Security Centre

2309120122-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Vulnerability in remote access VPN feature of Cisco device software - CVE-2023-20269

Wednesday 13th September, 2023

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Cisco has released a security advisory on a zero-day vulnerability, which is currently being exploited in the wild. This vulnerability currently affects the remote access VPN feature of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) software. The vulnerability is tracked as CVE-2023-20269. This could enable an unauthenticated, remote attacker to conduct brute force attacks or an authenticated, remote attacker to establish a clientless SSL VPN session with an unauthorised user.

In advance of a fixed software release, Cisco has provided workarounds and recommendations for organisations to mitigate against the vulnerability as well as indicators of compromise that might point to successful exploitation.

Further information can be found in Cisco's security advisory:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC

Products Affected

Cisco devices may be vulnerable based on their configuration. It is recommended that affected users review their device's configuration to determine if the device is vulnerable.

Alternatively, customers can determine their exposure to vulnerabilities in Cisco ASA and FTD Software by using the Cisco Software Checker. This tool identifies any Cisco security advisories that impact a specific software release.

Cisco software checker: https://sec.cloudapps.cisco.com/security/center/softwarechecker.x

Impact

A successful exploit could allow an attacker to achieve one or both of the following:

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

Cisco is aware of reports of this vulnerability being actively exploited in the wild. Further information can be found in Cisco's blog relating to this.

https://blogs.cisco.com/security/akira-ransomware-targeting-vpns-without-multi-factor-authentication

Recommendations

This vulnerability does not allow an attacker to bypass authentication, highlighting the importance of enabling Multi Factor Authentication whenever possible.

The NCSC strongly advises affected organisations to identify any Cisco devices that are running Cisco ASA or FTD software and use the Cisco software checker tool to identify vulnerable instances.

Cisco's workarounds and recommendations should then be implemented to mitigate against the vulnerability. Cisco's listed indicators of compromise should also be reviewed to confirm a successful exploitation.

Further information and steps that organisations can take can be found here:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC
- https://sec.cloudapps.cisco.com/security/center/softwarechecker.x

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie