UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00219

CISCO ASA & FIREPOWER ALLOW SECURITY BYPASS

DATE ISSUED: 1st November 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

Cisco's Adaptive Security Appliances (ASA) and FirePower Threat Defence (FTD) software could allow attackers to bypass security mechanisms on the systems but as yet, there are no reports of active attacks in the wild.

BREAKDOWN

As the result of a design error in the identity-based firewalls rule processing feature, an unauthenticated attacker could bypass security controls on the targeted Cisco device. The vulnerability is currently being tracked as CVE-2021-34787. An attacker could send a specially crafted network request to the affected device to gain access and control of the device to carry out attacks on connected devices, eavesdrop or disrupt network services. Affected devices include ASA Software prior to 9.16.1.28 and Cisco FirePower Threat Defence Software prior to 7.0.1

REMEDIATION STEPS

- Apply the security patches provided by Cisco that are relevant to your device and current installed version after appropriate testing has been completed.
- To diminish a successful attack all software should be run as a non-privileged user
- Educate users on the dangers of visiting unknown or untrusted websites
- Educate users on the dangers associated with phishing emails, particularly those containing hyperlinks and attachments and what to do with any suspicious emails within your organisation.
- Check users only have access and privileges relevant to their role and remediate where necessary using the principles or least-access, least privilege, and need-to-know

REFERENCES & RESOURCES

CVE	https://www.cve.org/CVERecord?id=CVE-2021-34787
Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY
CIS Advisory	