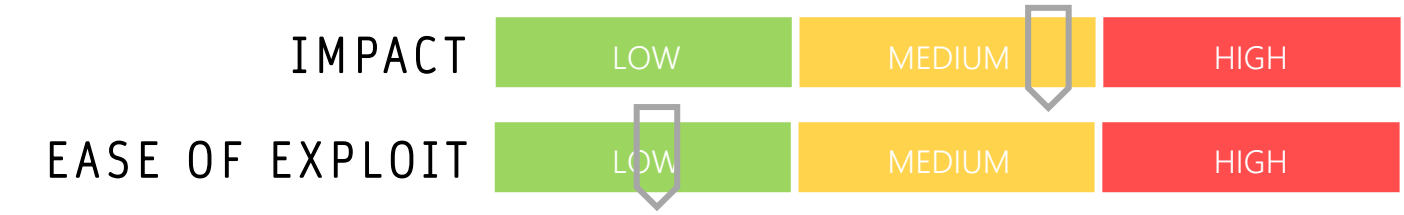
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00017

CISCO NETWORK SECURITY FLAW

DATE ISSUED: 27th July 2020



OVERVIEW

Patches are now available for the vulnerability CVE-2020-3452 but attackers are still actively targeting and exploiting vulnerable, un-patched software versions with the high-severity flaw allowing remote access to unauthenticated users in its network security software.

BREAKDOWN

Targeting the web interface services for FirePower Threat Defence (FTD) and network operating system of their Adaptive Security Appliances (ASA) present a flaw relating to input validation of URLs in HTTP requests. Using the HTTP based directory traversal type of attack, malicious actors are able to gain access to privileged directories and execute commands outside of the web server's directory. Sensitive files may be read by attackers within the web service file system, which are enabled by default when using WebVPN or AnyConnect services, including information such as the WebVPN configurations, web cookies, bookmarks, history and HTTP URLs, The attacked will be unable to gain access to underlying operating system files.

REMEDIATION STEPS

- Immediately patch and reboot any affected devices
- Monitor network logs for unusual activity
- Any ASA devices with software versions 9.7 and earlier or FTD release 6.2.2 and earlier have reached end of life for maintenance support and should be upgraded or replaced as soon as possible.

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/attackers-exploiting-high-severity-network-security-flaw-cisco-warns/157756/
NIST https://nvd.nist.gov/vuln/detail/CVE-2020-3452
Cisco https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ro-path-KJuQhB86
Tenable https://www.tenable.com/blog/cve-2020-3452-cisco-adaptive-security-appliance-and-firepower-threat-defense-path-traversal