UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00025

CISCO CRITICAL VWAN FLAW

DATE ISSUED: 22nd August 2020

IMPACT	LOW	[✓ MEDIUM]	HIGH
EASE OF EXPLOIT	LOW	[✓ MEDIUM]	HIGH

OVERVIEW

A flaw granting administrative access to remote, unauthenticated users may be present in the Cisco ENCS 5400-W Series and CSP 5000-W Series running Cisco virtual Wide Area Application Services (vWAAS). This purpose of this software being WAN optimization to assist in managing business applications in private cloud infrastructure. CVE-2020-3446.

BREAKDOWN

Default passwords linked to user accounts for software may be obtained by an unauthorised user that may be used to escalate privileges to the administration level. The Cisco Enterprise Network Compute Series (ENCS) hardware appliances are used to deploy the Cisco Enterprise NFV Infrastructure Software (NFVIS) for complete management of virtualised service. Attackers would need to be able to access the command line interface (CLI) of an affected device in order to exploit this vulnerability.

REMEDIATION STEPS

- Install security update patch released by Cisco on any affected devices in the ENCS series with v6.4.5 or 6.4.3d and earlier NFVIS software
- Monitor network for suspicious activity
- Scan devices using anti-malware software to detect any running malware

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/cisco-critical-flaw-patched-in-wan-software-solution/158485/
Latest Hacking News:	https://latesthackingnews.com/2020/08/21/cisco-patched-critical-vulnerability-in-cisco-vwaas/
SDX Central	https://www.sdxcentral.com/articles/news/cisco-patches-critical-wan-software-bug/2020/08/