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

CYBER GUIDANCE ISSUE 00045

CISCO TACKLES 29 HIGH-SEVERITY BUGS

DATE ISSUED: 28th September 2020

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

OVERVIEW

Cisco has recently released a group of patches to address the existing flaws on a number of networking devices that run their proprietary Cisco IOS XE software.

BREAKDOWN

Two of the most risky vulnerabilities addressed in this mass release relate to the Zone-Based Firewall (CVE-2020-3421 & CVE-2020-3480) along with a few others that also allow remote, unauthorised access. These included a web User Interface (UI) bypass, DoS conditions caused by devices being forced to reload and other local an adjacent attacks. Such attacks include Remote Code Execution (RCE) in various forms and persistent code execution.

CVE-2020-3417, CVE-2020-3418, CVE-2020-3509, CVE-2020-3559

REMEDIATION STEPS

- Update all Citrix Workspace App for Windows to the latest version
- Monitor networks for unusual activities, sharing and downloads

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/cisco-patches-bugs/159537/
CVE Details	https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-19/Cisco-IOS.html