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

CYBER GUIDANCE ISSUE 00160

CISCO 220 SMART SWITCH VULNERABILITIES

DATE ISSUED: 21st June 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A number of vulnerabilities have been discovered in Cisco's 220 Series Smart Switches for small business affecting firmware versions prior to 1.2.0.6 with the web-based management interface enabled.

BREAKDOWN

The first CVE-2021-1542 allows a remote attacker to take over a user's session to gain access to the switches web portal where they may then escalate their privileges. Another CVE-2021-1541 allows an attacker with administrative access to remotely execute root-privileged commands on the operating system. Further vulnerabilities include CVE-2021-1543 and CVE-2021-1571 which allows an attacker to initiate remote Cross Site Scripting (XSS) or HTML injection attacks. During testing, a researcher also found that CVE-2021-1543 may also be used to include a Javascript payload to deploy malicious code.

REMEDIATION STEPS

- Apply the latest security patches issued by Cisco to all affected switches.
  - 220 Serie Smart Switches
  - Historical vulnerabilities exist for the 200 & 250 Series Smart switches, 300, 350 & 350X Series Managed Switches, 500 & 550X series.

REFERENCES & RESOURCES

E Hacking News	https://www.ehackingnews.com/2021/06/cisco-smart-switches-detected-with.html
Security Week	https://www.securityweek.com/researcher-finds-several-vulnerabilities-cisco-small-business-switches
Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E
CIS	https://www.cisecurity.org/advisory/a-vulnerability-with-cisco-small-business-smart-and-managed-switches-could-allow-for-denial-of-service_2020-119/