NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

June 2021, Edition 1.0

NETWORK INTELLIGENCE SECURITY ADVISORY

The major security news items of the month - major threats and security patch advisory. The advisory also includes IOCs and remediation steps.

IN THIS EDITION:

Security Advisory Listing	Severity
Multiple high severity vulnerabilities in Cisco Products were more likely to be exploited in Malware attacks and Hacking campaigns	🟠 High
Threat Actor Group Andariel were found targeting various industrial sectors in South Korea with custom ransomware	🔴 Critical
An APT Threat Actor Group Gelsemium are actively conducting cyber-espionage campaigns targeting various critical organizations	🔴 Critical

ALSO INSIDE

Security Patch Advisory

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

Multiple high severity vulnerabilities in Cisco Products were more likely to be exploited in Malware attacks and Hacking campaigns

Severity: High

Date: June 18, 2021

IMPACT

Successful exploitation of these vulnerabilities (CVE-2021-1541, CVE-2021-1542, CVE-2021-1543 CVE-2021-1571, CVE-2021-1567, CVE-2021-1566 and CVE-2021-1134) allow remote attackers to gain unauthorized access, perform session hijacking, cross-site scripting (XSS) attack, HTML injection attack, MITM attack, execute arbitrary program/malicious code on the underlying operating system with elevated privileges in context of user account.

INTRODUCTION

Multiple vulnerabilities (CVE-2021-1541, CVE-2021-1542, CVE-2021-1543 & CVE-2021-1571) in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to Hijack a user session, Execute arbitrary commands as a root user on the underlying OS, Conduct a cross-site scripting (XSS) attack & HTML injection attack. These vulnerabilities affect only Cisco Small Business 220 Series Smart Switches that have the web-based management interface enabled.

RCE Vulnerability (CVE-2021-1541) exists in the web-based management interface of Cisco Small Business 220 Series Smart Switches. The vulnerability exists due to a lack of parameter validation for TFTP configuration parameters. An attacker could exploit this vulnerability by entering crafted input for specific TFTP configuration parameters. A successful exploit could allow the attacker to execute arbitrary commands as a root user on the underlying operating system. This is a post-authentication vulnerability.

Session Management Vulnerability (CVE-2021-1542) exists in Cisco Small Business 220 Series Smart Switches, it allows a remote attacker to bypass the authentication process. This vulnerability exists due to the use of weak session management for session identifier values. An attacker could exploit this vulnerability by using reconnaissance methods to determine how to craft a valid session identifier. A successful exploit could allow the attacker to take actions within the management interface with privileges up to the level of the administrative user.

Cross-Site Scripting (XSS) Vulnerability (CVE-2021-1543) exists in Cisco Small Business 220 Series Smart Switches. This vulnerability exists due to insufficient sanitization of user-supplied data by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user to click a malicious link and access a specific page. A successful the exploit could allow an unauthenticated remote attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information and redirect the user to an arbitrary page.

HTML Injection Vulnerability (CVE-2021-1571) exists in Cisco Small Business 220 Series Smart Switches. This vulnerability is due to improper checks of parameter values in affected pages. An unauthenticated attacker could exploit this vulnerability by persuading a user to follow a crafted link that is designed to pass HTML code into an affected parameter. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites.

DLL Hijacking Vulnerability (CVE-2021-1567) existing in Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack. This vulnerability exists due to the application loads DLL libraries in an insecure manner. An attacker could exploit this vulnerability by sending a series of crafted interprocess communication (IPC) messages to the AnyConnect process.

Multiple high severity vulnerabilities in Cisco Products were more likely to be exploited in Malware attacks and Hacking campaigns

Severity: High

Date: June 18, 2021

RECOMMENDATIONS

1. Update Cisco Small Business 220 Series Smart Switches firmware to releases 1.2.0.6 and later

2. Update Cisco AnyConnect Secure Mobility Client for Windows to releases 4.10.01075 and later

3. Update Cisco AsyncOS to fixed releases 12.5.3-035, 13.0.0-030, 13.5.3-010, 11.8.3-021, 12.0.3- 005 and 12.5.1-043

4. Update Cisco DNA Center Software to releases 2.2.2.1 and 2.2.2.3 and later

A successful exploit could allow the attacker to execute arbitrary code on the affected device with SYSTEM privileges. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. It’s only exploitable if the VPN Posture (HostScan) Module is installed on the AnyConnect client.

Certificate Validation Vulnerability (CVE-2021-1566) exists in Cisco Email Security Appliance (ESA) and Cisco Web Security Appliance (WSA). This vulnerability exists due to improper certificate validation when establishing TLS connection. A man-in-the-middle attacker could exploit this vulnerability by sending a crafted TLS packet to an affected device. A successful exploit could allow the attacker to spoof a trusted host and then extract sensitive information or alter certain API requests.

Certificate Validation Vulnerability (CVE-2021-1134) exists in Cisco DNA Center. This vulnerability exists due to an incomplete validation of the X.509 certificate used when establishing a connection between DNA Center and Cisco Identity Services Engine (ISE) server. An unauthenticated attacker could exploit this vulnerability by supplying a crafted certificate and could then intercept communications between the ISE and DNA Center. A successful exploit could allow the attacker to view and alter sensitive information that the ISE maintains about clients that are connected to the network.

AFFECTED COMPONENTS

- Cisco Small Business 220 Series Smart Switches running firmware releases earlier than Release 1.2.0.6
- Cisco AnyConnect Secure Mobility Client for Windows releases earlier than Release 4.10.01075
- Cisco DNA Center Software Releases earlier than 2.2.2.1
- Cisco Email Security Appliance running Cisco AsyncOS versions 12.5, 13.0, 13.5 and earlier than 12.5
- Cisco Web Security Appliance running Cisco AsyncOS versions 11.8, 12.0, 12.5, earlier than 11.8

READ

- Cisco Smart Switches Riddled with Severe Security

Threat Actor Group Andariel were found targeting various industrial sectors in South Korea with custom ransomware

Severity: Critical

Date: June 17, 2021

URL

hxxp://ddjm[.]co[.]kr/bbs/icon/skin/skin[.]php
hxxp://hivekorea[.]com/jdboard/member/list[.]php
hxxp://mail[.]namusoft[.]kr/jsp/user/eam/board[.]jsp
hxxp://mail[.]sisnet[.]co[.]kr/jsp/user/sms/sms_recv[.]jsp
hxxp://snum[.]or[.]kr/skin_img/skin[.]php
hxxp://www[.]allamwith[.]com/home/mobile/list[.]php
hxxp://www[.]conkorea[.]com/cshop/banner/list[.]php
hxxp://www[.]ddjm[.]co[.]kr/bbs/icon/skin/skin[.]php
hxxp://www[.]jinjinpig[.]co[.]kr/Anyboard/skin/board[.]php

IP’s

198.55.119[.]112
45.58.112[.]77
23.229.111[.]197
23.229.111[.]197
185.208.158[.]208

REMEDIATION

1. Block the threat indicators at their respective controls.
2. Ensure Microsoft Windows Workstations are updated with the latest security patches.
3. Ensure Microsoft Exchange Server and Microsoft IIS Server are updated with the latest security patches.
4. Ensure Linux workstations & servers are updated with the latest security patches.
5. Do not click on links or download untrusted email attachments coming from unknown email addresses.
6. Ensure Domain Accounts follows the least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.
7. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through a VPN tunnel.
8. Enable User Account Control (UAC) to mitigate the impact of malware.
9. Keep all systems and software updated to the latest patched versions.
10. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
11. Monitor DNS traffic for irregular requests & responses moving in and out of network.
12. Ensure data backup is done periodically and ensure data backups are done via an out-of-band network onto the server with limited or no internet access.
13. Limit unnecessary lateral communications between network hosts, segments, and devices.
14. Ensure to monitor suspicious activity or intrusion through SIEM solution.

READ

- Andariel evolves to target South Korea with ransomware
- Andariel Group Targets South Korean Entities in New Campaign
- Lazarus APT conceals malicious code within BMP image to drop its RAT

Threat Actor Group Andariel were found targeting various industrial sectors in South Korea with custom ransomware

Severity: Critical

Date: June 17, 2021

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
f1eed93e555a0a33c7fef74084a6f8d06a92079e9f57114f523353d877226d72	Yes	Yes	Yes	Yes	Yes
79e15cc02c6359cdb84885f6b84facbf91f6df1254551750dd642ff96998db35	Yes	Yes	Yes	Yes	Yes
a6ed3fe39d0956182c0ba9b57966cb8ae84ea029aa8d726f5bef9e7637f549f8	Yes	Yes	Yes	Yes	Yes
0193bd8bcbce9765dbecb288d46286bdc134261e4bff1f3c1f772d34fe4ec695	Yes	Yes	Yes	Yes	Yes
0996a8e5ec1a41645309e2ca395d3a6b766a7c52784c974c776f258c1b25a76c	Yes	Yes	Yes	Yes	Yes
ed5fbefd61a72ec9f8a5ebd7fa7bcd632ec55f04bdd4a4e24686edccb0268e05	Yes	Yes	Yes	Yes	Yes
2dff6d721af21db7d37fc1bd8b673ec07b7114737f4df2fa8b2ecfffbe608a00	Yes	Yes	Yes	Yes	Yes
6310cd9f8b6ae1fdc1b55fe190026a119f7ea526cd3fc22a215bda51c9c28214	Yes	Yes	Yes	Yes	Yes
b59e8f44822ad6bc3b4067bfdfd1ad286b8ba76c1a3faff82a3feb7bdf96b9c5	Yes	Yes	Yes	Yes	Yes
ab194f2bad37bffd32fae9833dafaa04c79c9e117d86aa46432eadef64a43ad6	Yes	Yes	Yes	Yes	Yes
f4765f7b089d99b1cdcebf3ad7ba7e3e23ce411deab29b7afd782b23352e698f	No	No	No	No	No
f6ab4e92dadd831dbc02a3cc27d2f6aee4f39e1743485638c8aa2c09341eda49	Yes	Yes	Yes	Yes	Yes
1177105e51fa02f9977bd435f9066123ace32b991ed54912ece8f3d4fbeeade4	Yes	yes	Yes	yes	Yes
4da0ac4c3f47f69c992abb5d6e9803348bf9f3c6028a7214dcabec9a2e729b99	Yes	Yes	Yes	Yes	Yes
9137e886e414b12581852b96a1d90ee875053f16b79be57694df9f93f3ead506	Yes	Yes	Yes	Yes	Yes

An APT Threat Actor Group Gelsemium are actively conducting cyber-espionage campaigns targeting various critical organizations

Severity: Critical

Date: June 16, 2021

DOMAINS

4vw37z[.]cn
acro.ns1[.]name
domain.dns04[.]com
info.96html[.]com
microsoftservice.dns1[.]us
pctftp.otzo[.]com
sitesafecdn.hopto[.]org
traveltime.hopto[.]org
www.sitesafecdn.dynamic-dns[.]net
www.travel.dns04[.]com

IP's

149.248.14[.]53
210.209.72[.]180

REMEDIATION

1. Block the threat indicators at their respective controls.
2. Ensure Microsoft Windows Workstations are updated with the latest security patches.
3. Ensure Microsoft Exchange Server and Microsoft IIS Server are updated with the latest security patches.
4. Ensure Linux workstations & servers are updated with the latest security patches.
5. Do not click on links or download untrusted email attachments coming from unknown email addresses.
6. Ensure Domain Accounts follows the least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.
7. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through a VPN tunnel.
8. Enable User Account Control (UAC) to mitigate the impact of malware.
9. Keep all systems and software updated to the latest patched versions.
10. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
11. Monitor DNS traffic for irregular requests & responses moving in and out of the network
12. Ensure data backup is done periodically and ensure data backups are done via an out-of-band network onto the server with limited or no internet access.
13. Limit unnecessary lateral communications between network hosts, segments, and devices.
14. Ensure to monitor suspicious activity or intrusion through SIEM solution.

READ

- Gelsemium: When threat actors go gardening
- Gelsemium Hacker Group Attack Governments, Universities Using Various Hacking Tools
- NoxPlayer Supply-Chain Attack is Likely the Work of Gelsemium Hackers

An APT Threat Actor Group Gelsemium are actively conducting cyber-espionage campaigns targeting various critical organizations

Severity: Critical

Date: June 16, 2021

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
00b701e3ef29912c1fcd8c2154c4ae372cfe542cfa54ffcce9fb449883097cec	Yes	Yes	Yes	Yes	Yes
0112ca2cae2d70098c3801f5f36b261573bb115a2b005b4e98a1ca12f7b64625	No	No	No	No	No
0ba328cd38e89362db42c756ea25f2e159ad2aa502e0ad7ce2226fda485e2c4c	No	No	No	No	No
0c94a6e24104e6bdeac00715ade268dd7d80b1baadda23bd50708d28ed1de025	No	No	No	No	No
109d4b8878b8c8f3b7015f6b3ae573a6799296becce0f32ca3bd216bee0ab473	Yes	Yes	Yes	Yes	Yes
171cddae21cf41e6d36c1e3d33d0bd79f55f4d3d2d9a35faa8f1c210c8779cfa	No	No	No	No	No
1827f58b41c2f3a2a3fb425be0d43d0b3c5e52f3edefee77284864a6db132bb9	No	No	No	No	No
1a9d78e5c255de239fb18b2cf47c4c2298f047073299c27fb54a0edf08a1d5a1	Yes	Yes	Yes	Yes	Yes
1b6bb9e9612982f9cb55a1c88ae988d362d03fd57748d10b8cbe7acd724055c9	No	No	No	No	No
1f6de1af513f60572799a0893818e1b694c3ec3ff5dabddc8a0f0aa0d96d15d2	No	No	No	No	No
f4765f7b089d99b1cdcebf3ad7ba7e3e23ce411deab29b7afd782b23352e698f	No	No	No	No	No
29e78ca3cb49dd2985a29e74cafb1a0a15515670da0f4881f6095fb2926bfefd	Yes	Yes	Yes	Yes	Yes
31d5e55f21246f97da006ddba6306b357d2823c90754a920c7bd268af0d2a1e4	No	No	No	No	No
353f168aef1a1bbf4844bf4a01d592db3a761aa4ea7355b0d8c8bc27ea03bea2	No	No	No	No	No
35426c457011cc5955d9d1395a810edc6731629260daffc9eaba8448f8676a25	No	No	No	No	No

Security Patch Advisory

14th June to 20th June | Trac- ID: NII21.06.0.3

Severity Matrix			
🟩 L	🟨 M	🟧 H	🟥 C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
🟩 June 15, 2021	Ubuntu Linux	USN-4988-1: ImageMagick vulnerabilities	▪ Ubuntu 20.10 ▪ Ubuntu 20.04 LTS ▪ Ubuntu 18.04 LTS	Kindly update to fixed version
🟨 June 16, 2021	Ubuntu Linux	USN-4989-1: BlueZ vulnerabilities	▪ Ubuntu 21.04 ▪ Ubuntu 20.10 ▪ Ubuntu 20.04 LTS ▪ Ubuntu 18.04 LTS	Kindly update to fixed version

RED HAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
🟧 June 15, 2021	Red Hat Enterprise Linux	RHSA-2021:2445	▪ Red Hat Enterprise Linux Server 7 x86_64 ▪ Red Hat Enterprise Linux for x86_64 8 x86_64	Kindly update to fixed version
🟧 June 17, 2021	Red Hat Enterprise Linux	RHSA-2021:2467	▪ Red Hat Enterprise Linux Server - Extended Life Cycle Support 6 x86_64 ▪ Red Hat Enterprise Linux Server - Extended Life Cycle Support 6 i386	Kindly update to fixed version

Security Patch Advisory

14th June to 20th June | Trac- ID: NII21.06.0.3

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

ORACLE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
June 14, 2021	Oracle Linux	ELSA-2021-9305 - Unbreakable Enterprise kernel security update	▪ Oracle Linux 7 (aarch64) ▪ Oracle Linux 7 (x86_64)	Kindly update to fixed version
June 14, 2021	Oracle Linux	ELSA-2021-2206 - firefox security update	▪ Oracle Linux 8 (aarch64) ▪ Oracle Linux 8 (x86_64)	Kindly update to fixed version

NETAPP

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
June 14, 2021	NetApp Products	August 2020 Apache HTTP Server Vulnerabilities in NetApp Products	• None of te products are affected.	Kindly update to fixed version
June 14, 2021	NetApp Products	CVE-2020-24509 Intel SPS Vulnerability in NetApp Products	• None of the products are affected.	Kindly update to fixed version