NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

September 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
BulletProofLink, a large-scale phishing-as-a-service (PhaaS) operation driving many phishing campaigns are targeting corporate organizations.	High
Watchdog group (aka, Golden-Eyed Dog) found targeting Merchants and Shareholders,with remote access trojans.	High
Threat actors in the latest ongoing campaign, are actively targeting taxpayers in India using new android malware Elibomi.	High
An authentication bypass vulnerability (CVE-2021-34746) in Cisco Enterprise NFV Infrastructure Software allows attacker to gain administrator access.	Critical
Threat actors are deploying new Mirai malware variants, in one of their latest campaigns by exploiting recently disclosed WebSVN Command Injection Vulnerability.	High

ALSO INSIDE

Security Patch Advisory

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

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

BulletProofLink, a large-scale phishing-as-a-service (PhaaS) operation driving many phishing campaigns are targeting corporate organizations.

Severity: High

Date: September 23, 2021

DOMAINS

apidatacss[.]com
apiserverdata1[.]com
baller[.]top
datacenter01.us
f1smtp[.]com
f1smtp[.]com
gpxsmtp[.]com
gurl101[.]services
hostprivate[.]us
josmtp[.]com
link101[.]bid
linuxsmtp[.]com
migration101[.]us
panelsmtp[.]com
racksmtp[.]com
rosmtp[.]com
rxasmtp[.]com
thegreenmy87[.]com
vitme[.]bid
voksmtp[.]com
winsmtp[.]com
trasactionsmtp[.]com
moneysmtp[.]com
foxsmtp[.]com

REMEDIATION

1. Block the threat indicators at their respective controls.
2. Ensure Microsoft Windows Workstations, Microsoft Exchange Server and Microsoft IIS Server are updated with the latest security patches.
3. Do not click on links or download untrusted email attachments coming from unknown email addresses.
4. Ensure Domain Accounts follows the least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.
5. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through a VPN tunnel.
6. Keep all systems and software updated to the latest patched versions.
7. Use Microsoft's Enhanced Mitigation Experience Toolkit (EMET) to block methods of using trusted binaries to bypass application control.
8. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
9. Ensure Remote Desktop (RDP), Remote Procedure Call (RPC), and Virtual Network Computing (VNC) Services are strictly isolated from internet-facing cloud or on-premise IT infrastructure. And ensure these remote services are only allowed through VPN tunnels.
10. Limit unnecessary lateral communications between network hoses, segments, and devices.
11. Implement unauthorized execution prevention by disabling macro scripts from Microsoft Office files, monitor and/or block inbound connections from Tor exit nodes and other anonymization services.

URL's

hxxps<://>Faileduebpicture.cc/email-list/finish-unv2[.]php
hxxps<://>Failedsendapidata[.]com/email-list/finish-unv2[.]php
hxxps<://>webpicture.cc/email-list/finish-unv2[.]php?phishing-processor
hxxps<://>prvtsmtp[.]com/email-list/finish-unv2[.]php
hxxps<://>webpicture.cc/email-list/finish-unv2.ph
hxxps<://>apiserverdata1[.]com/email-list/finish-unv2[.]php
hxxps<://>sendapidata[.]com/email-list/finish-unv2[.]php
hxxps<://>apidatacss[.]com/finish-unv22[.]php
hxxps<://>ses-smtp[.]com/email-list/office19999999/finish[.]php
hxxps<://> ses-smtp[.]com/email-list/onedrive25/finish[.]php
hxxps<://> ses-smtp[.]com/email-list/office365nw/finish[.]php
hxxps<://>smtpro101[.]com/email-list/onedrive25/finish[.]php
hxxps<://>smtpro101[.]com/email-list/office19999999/finish[.]php
hxxps<://>plutosmto[.]com/email-list/office365nw/finish[.]php

READ

- Phishing-as-a-service operation uses double theft to boost profits
- Catching the big fish: Analyzing a large-scale phishing-as-a-service operation

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Watchdog group (aka, Golden-Eyed Dog) found targeting Merchants and Shareholders, with remote access trojans.

Severity: High

Date: September 23, 2021

IP ADDRESSES

144.48.8.72
43.252.231.58
192.253.239.93
58.221.42.59

DOMAINS

ouyipay.net
hlsypay.com

URLS

ouyipay.net
hlsypay.com

REMEDIATION

1. Ensure Microsoft Windows Servers and Workstations are updated with the latest security patches.
2. Ensure Microsoft Exchange Server and Microsoft IIS Server are updated with latest security patches.
3. Ensure proper network segmentation are done, and ensure communication through TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are explicitly allowed on-demand only for particular network segments when needed.
4. Ensure network segments that allow communication over TCP port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are strictly monitored for any anomaly or suspicious patterns like lateral movement, excessive network traffics on TCP port 135, TCP Port 445, TCP Port 1900, TCP Port 3389, and an unusual amount of data transmission, etc.
5. Ensure Domain Accounts follows the least privilege principle and ensure two-factor authentication is enabled on all Business Email Accounts.
6. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through a VPN tunnel.
7. Ensure VPN client software and VPN servers are patched with the latest security updates released by the vendor.
8. Strictly ensure TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are not left open on the Internet or DMZ facing side.
9. Please ensure TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389, are only accessible through VPN tunnels between VPN clients and Organization's Resources.
10. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
11. Ensure to monitor for excessive LDAP queries within 5 minutes from particular the system, via SIEM solution.
12. Ensure VNC, SOCKS, and SMTP ports are also closely monitored.
13. 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.
14. Kindly Block IP, Domain, URLs, and Hashes, on the perimeter security devices.

READ

- "Watchdog" group phishing attacks on merchants

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Threat actors in the latest ongoing campaign, are actively targeting taxpayers in India using new android malware Elibomi.

Severity: High

Date: September 06, 2021

REMEDIATION

1. Block the threat indicators at their respective controls.
2. Disable “Install unknown apps” in android settings (this option is disabled in android by default).
3. Update applications and android security patches as soon as officially released.
4. Ensure the least required permissions are allowed for applications and ensure to not blindly allow all the permissions the application prompts.
5. Do not click on links or download third-party applications through SMS/emails pretending to be appearing on behalf of the Income Tax Department.
6. Don’t try to download and install hacked versions of applications, as most of them are infected.
7. Use a mobile security solution to monitors the device itself by constantly scanning network connections to detect malicious behaviors.

READ

- Phishing Android Malware Targets Taxpayers in India

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
e6f20e73af6cc393dd139b32117a8681e15edfe61c157f3509d1e740184b3d5c	Yes	Yes	Yes	No	Yes
c782f9cdec637503472bc62d25348cefccc3de58244441547f3e2ed9b22c6c93	Yes	Yes	Yes	No	Yes
63c2cae1f3d04d81a4a1dcd773c62d7e9a71cf7e3ae0c5a9f931353e86f11651	yes	Yes	Yes	No	yes
3cc3d7d32e8c85e0c594ca5cb2ecfbfba66ebbc1853bcb02c2a39fce9f238dbc	Yes	Yes	Yes	No	Yes
dc7cf2212f09482ac034eb7e9f89ef0cec8bc9532d4fe2db8a880c2e1e4ee8a2	Yes	Yes	Yes	No	Yes
8cc43db17480170fac3213518fe18d52a5648ce04060561d6359d6c589a4321c	Yes	Yes	Yes	No	Yes
b09c85e75f65a9acc4693957caf4b4c56dd808c7d0d657c1bc9f74a1bd772abe	Yes	Yes	Yes	No	Yes
a55a2318e95dcfbe2d2082ee569642034ab05168fa0142ff1009798131b61f52	Yes	Yes	No	No	Yes
b43fd19dfeeb89507f9de162e7a727fa6024ca4b1d19cb5c44e53755200f2b66	Yes	Yes	No	No	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

An authentication bypass vulnerability (CVE-2021-34746) in Cisco Enterprise NFV Infrastructure Software allows attacker to gain administrator access.

Severity: Critical

Date: September 02, 2021

BUSINESS IMPACT

Successful exploitation of this vulnerability could allow remote attacker to bypass authentication and login as an administrator to the affected device.

REMEDIATION

1. Kindly apply latest security patches to Cisco Enterprise NFV Infrastructure Software.

INTRODUCTION

An authentication bypass vulnerability (CVE-2021-34746) in the TACACS+ authentication, authorization and accounting (AAA) feature of Cisco Enterprise NFV Infrastructure Software allows a remote attacker to gain administrator access onto the affected Cisco devices.

This vulnerability is due to incomplete validation of user-provided input that is passed to an authentication script. The remote attacker could exploit this vulnerability by injecting parameters into an authentication request. On successful exploitation of this vulnerability, could allow a remote attackers to bypass authentication and login as an administrator to the affected device.

VULNERABLE PRODUCT

This vulnerability affects Cisco Enterprise NFVIS Release 4.5.1 if the TACACS external authentication method is configured.

• To determine if a TACACS external authentication feature is enabled on a device, use the show running-config tacacs-server command.
• If the output of the show running-config tacacs-server command is No entries found the TACACS external authentication feature is not enabled.

• Alternatively, check the configuration through the GUI. Choose Configuration > Host > Security > User and Roles. If a TACACS+ host is defined under External Authentication, the device is considered to be vulnerable.

AFFECTED INDUSTRIES

Managed IT Service Providers

READ

- Cisco Enterprise NFV Infrastructure Software Authentication Bypas Vulnerability
- Cisco fixes a critical flaw in Enterprise NFVIS for which PoC exploit exists

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Threat actors are deploying new Mirai malware variants, in one of their latest campaigns by exploiting recently disclosed WebSVN Command Injection Vulnerability.

Severity: High

Date: September 01, 2021

IP

75.119.143[.]229

REMEDIATION

1. Block the threat indicators at their respective controls.
2. Ensure WebSVN is updated to latest software version.
3. Update Huawei/Realtek/GPON routers, Citrix ADC and D-Link products to latest versions.
4. Ensure SonicWall SSL-VPN is updated with latest security patches.
5. Ensure Microsoft Windows Workstations, Microsoft Exchange Server and Microsoft IIS Server are updated with latest security patches.
6. Ensure Linux workstation and servers are updated with latest security patches.
7. Ensure Domain Accounts follows least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.
8. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel.
9. Keep all systems and software updated to latest patched versions.
10. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
11. Ensure Remote Desktop (RDP), Remote Procedure Call (RPC), and Virtual Network Computing (VNC) Services are strictly isolated from internet facing cloud or on-premise IT infrastructure. And ensure these remote services are only allowed through VPN tunnels.
12. Limit unnecessary lateral communications between network hoses, segments, and devices.

READ

- New Mirai Variant Targets WebSVN Command Injection Vulnerability (CVE-2021-32305)

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Threat actors are deploying new Mirai malware variants, in one of their latest campaigns by exploiting recently disclosed WebSVN Command Injection Vulnerability.

Severity: High

Date: September 01, 2021

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
e6f20e73af6cc393dd139b32117a8681e15edfe61c157f3509d1e740184b3d5c	Yes	Yes	Yes	No	Yes
c782f9cdec637503472bc62d25348cefccc3de58244441547f3e2ed9b22c6c93	Yes	Yes	Yes	No	Yes
63c2cae1f3d04d81a4a1dcd773c62d7e9a71cf7e3ae0c5a9f931353e86f11651	yes	Yes	Yes	No	yes
3cc3d7d32e8c85e0c594ca5cb2ecfbfba66ebbc1853bcb02c2a39fce9f238dbc	Yes	Yes	Yes	No	Yes
dc7cf2212f09482ac034eb7e9f89ef0cec8bc9532d4fe2db8a880c2e1e4ee8a2	Yes	Yes	Yes	No	Yes
8cc43db17480170fac3213518fe18d52a5648ce04060561d6359d6c589a4321c	Yes	Yes	Yes	No	Yes
b09c85e75f65a9acc4693957caf4b4c56dd808c7d0d657c1bc9f74a1bd772abe	Yes	Yes	Yes	No	Yes
a55a2318e95dcfbe2d2082ee569642034ab05168fa0142ff1009798131b61f52	Yes	Yes	No	No	Yes
b43fd19dfeeb89507f9de162e7a727fa6024ca4b1d19cb5c44e53755200f2b66	Yes	Yes	No	No	Yes
7dc972346b9f82709bbcaabc30f126984468e60f2b085091471a9796ac4539b9	Yes	Yes	No	No	Yes
f4d851908e900d9201597f898cbb4420772a935901f25a77b31fc80e7cbc88b3	yes	Yes	Yes	No	Yes
889cc2a3e06c5770ff23017aa067cd8a01b8b410e143e9da63542ead7ce484da	Yes	Yes	Yes	No	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

6th September to 12th September | Trac- ID: NII21.09.0.2

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
September 10, 2021	Ubuntu Linux	USN-5075-1: Ghostscript vulnerability	• Ubuntu 21.04 • Ubuntu 20.04 LTS	Kindly update to fixed version

RED HAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
September 08, 2021	Red Hat JBoss Enterprise Application Platform	RHSA-2021:3471 - Security Advisory	▪ JBoss Enterprise Application Platform Text-Only Advisories x86_64	Kindly update to fixed version
September 08, 2021	Red Hat JBoss Enterprise Application Platform	RHSA-2021:3468 - Security Advisory	▪ JBoss Enterprise Application Platform 7.3 for RHEL 8 x86_64	Kindly update to fixed version

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

6th September to 12th September | Trac- ID: NII21.09.0.2

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

ORACLE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
September 10, 2021	Oracle Linux	ELSA-2021-9444 - oswatcher security update	▪ Oracle Linux 8 (aarch64) ▪ Oracle Linux 8 (x86_64) ▪ Oracle Linux 7 (aarch64) ▪ Oracle Linux 7 (x86_64)	Kindly update to fixed version
September 08, 2021	Oracle Linux	ELSA-2021-3447 - kernel security and bug fix update	▪ Oracle Linux 8 (aarch64) ▪ Oracle Linux 8 (x86_64)	Kindly update to fixed version

MOZILLA

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
August 18, 2021	Mozilla Thunderbird	Security Vulnerabilities fixed in Thunderbird 78.14	▪ Mozilla Thunderbird versions prior to 78.14	Kindly update to fixed version
August 18, 2021	Mozilla Thunderbird	Security Vulnerabilities fixed in Thunderbird 91.1	▪ Mozilla Thunderbird versions prior to 91.1	Kindly update to fixed version