NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

February 2022, 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
Chinese threat actors were found targeting critical organizations by deploying ShadowPad Malware in their ongoing cyberespionage campaigns.	High
Another Critical RCE bug (CVE-2022-24087) impacted Adobe Commerce and Magento Platforms.	Critical
A high-severity security bug (CVE-2022-20653) could allow attackers to crash Cisco ESA devices.	High
TA2541 threat actor group targeting aviation and other sensitive industries with various RAT's.	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

Chinese threat actors were found targeting critical organizations by deploying ShadowPad Malware in their ongoing cyberespionage campaigns.

Severity: High

Date: February 22, 2022

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. Ensure VPN client software and VPN servers are patched with the latest security updates released by the vendor.
7. Keep all systems and software updated to the latest patched versions.
8. Search for a subdirectory within C:\ProgramData, C:\Users\<username>\Roaming, or C:\Program Files that contain a legitimate executable (likely renamed) and one of the known ShadowPad DLL loader filenames (mscoree.dll, hpqhvsei.dll, secur32.dll, tosbtkbd.dll, log.dll, iviewers.dll) to identify possible ShadowPad compromise.
9. Hunt for a Windows service that launches the legitimate executable from the subdirectory containing the legitimate executable and one of the known ShadowPad DLL loaders to identify possible ShadowPad compromise.
10. When possible, include hash values in manifest files to help prevent side-loading of malicious libraries.
11. Ensure Remote Desktop (RDP), Remote Procedure Call (RPC), and Virtual Network Computing (VNC) Services are strictly isolated from the internet-facing cloud or on-premise IT infrastructure. And ensure these remote services are only allowed through VPN tunnels.
12. Ensure that unnecessary ports and services are closed to prevent the risk of discovery and potential exploitation.

DOMAINS

goest[.]mrbonus[.]com
phiinoc[.]dnsdyn[.]net
stratorpriv[.]lubni23[.]com
rolesnews[.]com
ti0wddsnv[.]wikimedia[.]vip
yjij4bpade[.]nslookup[.]club
Live[.]musicweb[.]xyz
Obo[.]videocenter[.]org
Teamview[.]Microsoft[.]msgloca
lmicro[.]com
Ts[.]ekaldhfl[.]club

IP's

47.56.228[.]89
5.188.33[.]106
139.180.141[.]16

READ

- ShadowPad Malware Analysis
- ShadowPad Modular Malware Platform Used by Chinese Hackers in High-profile Attacks
- Researchers Link ShadowPad Malware Attacks to Chinese Ministry and PLA

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Chinese threat actors were found targeting critical organizations by deploying ShadowPad Malware in their ongoing cyberespionage campaigns.

Severity: High

Date: February 22, 2022

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
69eb1aa0021c9b6905b8f0a354884a67f18d20aa045db20b5b5d59f41c7f201f	Yes	Yes	Yes	Yes	Yes
bc0c31be0d4784a6f8ad6333767580e61e7bbe500139fe0d111c39475470a312	Yes	Yes	Yes	Yes	Yes
0dfd91a0dd5d1143697413ebd50efde2411d07b4113d7d282ca0ec3c9d77d5ed	Yes	Yes	Yes	No	Yes
ec6852c341aff9d770debc1ef72fb5795c4d71c1327d57d79d65136cc2a670a4	Yes	Yes	Yes	No	Yes
dbb32cb933b6bb25e499185d6db71386a4b5709500d2da92d377171b7ff43294	Yes	Yes	Yes	Yes	Yes
18c4a15e587b223a3fb4d27eedeb16b81e5c75409d9ffbbe8aeeb7c4c2bd5041	Not Known	Not Known	Not Known	Not Known	Not Known
d8f695730fcf2cb5a894107740be0a0fa9bbae6851b83d396976a678236dec30	Yes	Yes	Yes	No	Yes
1402ed922a7efc05a6d9482136598fdb52afd95cb4e40190ea44a3ba087a58ab	No	No	No	No	No
8d1a5381492fe175c3c8263b6b81fd99aace9e2506881903d502336a55352fef	Yes	Yes	Yes	Yes	Yes
0371fc2a7cc73665971335fc23f38df2c82558961ad9fc2e984648c9415d8c4e	No	No	No	No	No
04089c1f71d62d50cbd8009dfd557aa1e6db1492a9fa2b35902182c07a0ed1c1	No	No	No	No	No

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Another Critical RCE bug (CVE-2022-24087) impacted Adobe Commerce and Magento Platforms.

Severity: Critical

Date: February 18, 2022

BUSINESS IMPACT

Successful exploitation of this the vulnerability allows a remote attacker to execute arbitrary code, inject digital skimmer, steal sensitive payment information, and completely compromise a vulnerable system.

RECOMMENDATIONS

1. Ensure to update Adobe Commerce and Magento Open Source products to latest security patches.

(Patch installation instructions – Click Here)

2. Monitor and Scan your Magento sites using Adobe's Magento Security Scan - Security Scan | Adobe Commerce 2.4 User Guide (magento.com)

INTRODUCTION

Adobe has addressed another critical Magento Zero-Day Vulnerability (CVE-2022-24087) that impacts Adobe Commerce and Magento Open Source products. It's a pre-authenticated remote code execution vulnerability that allows a remote attacker to execute arbitrary code and may result in the complete compromise of a vulnerable system.

The vulnerability exists due to improper input validation. A remote attacker can send a specially crafted request to the application and execute arbitrary code on the target system.

According to the researchers' estimations, there are more than 17,000 vulnerable websites, some of them from "major businesses."

The security bugs pose a potential risk of Magecart attacks, financial data theft, fraudulent transactions and financial harm, and full access to the target system with web-server privileges.

CVSS score: 9.8

AFFECTED PRODUCT

- Adobe Commerce 2.4.3-p1 and earlier versions, 2.3.7-p2 and earlier versions.
- Magento Open Source 2.4.3-p1 and earlier versions, 2.3.7-p2 and earlier versions.

Note: Adobe Commerce and Magento Open Source versions 2.3.0 to 2.3.3 are not affected.

READ

- Another Critical RCE Discovered in Adobe Commerce and Magento Platforms
- Researchers create exploit for critical Magento bug, Adobe updates advisory
- Security update available for Adobe Commerce | APSB22-12

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A high-severity security bug (CVE-2022-20653) could allow attackers to crash Cisco ESA devices

Severity: High

Date: February 18, 2022

BUSINESS IMPACT

Successful exploitation of this vulnerability allows a remote attacker to launch continuous DoS attacks and cause the device to become completely unavailable,resulting in a persistent DoS condition.

RECOMMENDATIONS

1. Ensure to update vulnerable Cisco AsyncOS Software to fixed software release.

WORKAROUND

1. Customers may configure bounce messages from Cisco ESA instead of from downstream dependent mail servers to prevent exploitation of this vulnerability.

(Note: Any workaround or mitigation that is implemented may negatively impact the functionality or performance of their network based on intrinsic customer deployment scenarios and limitations. Customers should not deploy any workarounds or mitigations before first evaluating the applicability to their own environment and any impact to such environment.)

INTRODUCTION

Cisco has addressed a high-severity security bug (CVE-2022-20653) in its Email Security Appliance (ESA) that could result in a denial-of-service (DoS) condition on an affected device.

The vulnerability exists in the DNS-based Authentication of Named Entities (DANE) email verification component of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA). The security flaw is due to insufficient error handling in DNS name resolution by the affected software. A remote non-authenticated attacker could exploit this vulnerability by sending specially crafted email messages to the affected device and performing a denial of service (DoS) attack.

CVSS score: 7.5

AFFECTED PRODUCT

- The vulnerability affects Cisco ESA devices running a vulnerable releases of Cisco AsyncOS Software with the DANE feature enabled and with the downstream mail servers configured to send bounce messages.

Vulnerable Cisco AsyncOS Software releases: 12.5 and earlier, 13.0, 13.5, 14.0

Note: Devices without the DANE feature enabled are not affected.
(To determine whether DANE is configured, check the web UI page **Mail Policies > Destination Controls > Add Destination** and verify whether the DANE Support option is enabled.)

READ

- Specially crafted emails could crash Cisco ESA devices
- Cisco Email Security Appliance DNS Verification Denial of Service Vulnerability

TA2541 threat actor group targeting aviation and other sensitive industries with various RAT's

Severity: High

Date: February 17, 2022

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. Inspect the sender email address in the header to ensure the address matches with the purported sender.
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. Keep all systems and software updated to the latest patched versions.
9. When possible, include hash values in manifest files to help prevent side-loading of malicious libraries.
10. Set PowerShell execution policy to execute only signed scripts. The change in policy on a system may be a way to detect malicious use of PowerShell.
11. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
12. Ensure Remote Desktop (RDP), Remote Procedure Call (RPC), and Virtual Network Computing (VNC) Services are strictly isolated from the internet-facing cloud or on-premise IT infrastructure. And ensure these remote services are only allowed through VPN tunnels.
13. Educate employees about phishing attacks and use effective email filtering techniques from external sources.
14. Disable Windows Script Host, this will prevent users from running any scripts (including VBScript and JScript scripts) that rely on WSH.
15. Monitor for Scheduled Tasks creation in the following paths: C:\Users\[User]\AppData\Local\Temp\tmp7CF8.tmp and C:\Users\[User]\AppData\Roaming\xubntzl.txt to detect the threat activity.
16. Ensure that unnecessary ports and services are closed to prevent the risk of discovery and potential exploitation.

DOMAINS

tq744[.]publicvm[.]com
e29rava[.]ddns[.]net
bodmas01[.]zapto[.]org
akconsult[.]ddns[.]net

joelthomas[.]linkpc[.]net
rick63[.]publicvm[.]com
h0pe[.]ddns[.]net
kimjoy[.]ddns[.]net

bigdips0n[.]publicvm[.]com
grace5321[.]publicvm[.]com

READ

- TA2541: APT Has Been Shooting RATs at Aviation for Years
- Charting TA2541's Flight

TA2541 threat actor group targeting aviation and other sensitive industries with various RAT's

Severity: High

Date: February 17, 2022

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
69eb1aa0021c9b6905b8f0a354884a67f18d20aa045db20b5b5d59f41c7f201f	Yes	Yes	Yes	Yes	Yes
bc0c31be0d4784a6f8ad6333767580e61e7bbe500139fe0d111c39475470a312	Yes	Yes	Yes	Yes	Yes
0dfd91a0dd5d1143697413ebd50efde2411d07b4113d7d282ca0ec3c9d77d5ed	Yes	Yes	Yes	No	Yes
ec6852c341aff9d770debc1ef72fb5795c4d71c1327d57d79d65136cc2a670a4	Yes	Yes	Yes	No	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

14th February to 22nd February | Trac- ID:NII22.02.0.3

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

ORACLE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
14-Feb-22	Ubuntu Linux	USN-5284-1: Firefox vulnerabilities	• Ubuntu 21.10 • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS	Kindly update to fixed version

RED HAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
14-Feb-22	Red Hat Enterprise Linux	RHSA-2022:0510 - Security Advisory	• Red Hat Enterprise Linux for x86_64 8 x86_64 • Red Hat Enterprise Linux for ARM 64 8 aarch64	Kindly update to fixed version
14-Feb-22	Red Hat Enterprise Linux	RHSA-2022:0530 - Security Advisory	• Red Hat Enterprise Linux Server - AUS 7.3 x86_64	Kindly update to fixed version

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

14th February to 22nd February | Trac- ID:NII22.02.0.3

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

ORACLE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
14-Feb-22	Oracle Linux	ELSA-2022-9148 - Unbreakable Enterprise kernel-container security update	▪ Oracle Linux 7 (aarch64) ▪ Oracle Linux 8 (x86_64)	Kindly update to fixed version
14-Feb-22	Oracle Linux	ELSA-2022-0510 - firefox security update	• Oracle Linux 8 (x86_64) • Oracle Linux 8 (x86_64)	Kindly update to fixed version

CENTOS

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
15-Feb-22	CentOS Linux	CentOS alert CESA-2022:0514 (firefox)	▪ CentOS 7 (x86_64)	Kindly update to fixed version