NETWORK INTELLIGENCE

The Digital Security Company

September 2022, Edition 1.0

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- Critical RCE bug in multiple Zoho ManageEngine products is being exploited in the wild
- Multiple Vulnerabilities in Microsoft Edge (Chromium based)
- American Airlines has suffered a data breach after falling victim to a phishing scam
- High-severity Privilege Escalation bug in pre-installed HP Support Assistant tool

Also Inside

Security Patch Advisory

Critical High Low

Date: September 23, 2022

Critical RCE bug in multiple Zoho ManageEngine products is being exploited in the wild

BUSINESS IMPACT

Successful exploitation of the vulnerability allows remote attackers to execute arbitrary code as the SYSTEM user, enter internal networks, compromise data on the server and crash or shut down the whole server and applications.

RECOMMENDATIONS

1. Download the latest upgrade pack and apply the latest build to your existing product installation as per the upgrade pack instructions from the following links for the respective product:
PAM360:
https://www.manageengine.com/privileged-accessmanagement/upgradepack.html
Password Manager Pro:
https://www.manageengine.com/products/passwordmanagerpro/upgradepack.html
Access Manager Plus:
https://www.manageengine.com/privileged-sessionmanagement/upgradepack.html

INTRODUCTION

Zoho has released fixes to address the remote code execution bug (CVE-2022-35405) in Zoho ManageEngine PAM360, Password Manager Pro, and Access Manager Plus.

CVE-2022-35405 is a deserialization vulnerability that causes unauthenticated RCE in XML-RPC of Zoho Manage Engine Password Manager Pro, PAM360 and authenticated RCE in XML-RPC of Access Manager Plus.

Unauthenticated attackers can send a crafted XML-RPC request containing malicious serialized data to /xmlrpc to gain remote command execution as the SYSTEM user.

Proof-of-concept (PoC) exploit code and a Metasploit module targeting this bug to gain RCE as the SYSTEM user has been publicly available online since August. The Metasploit module exploits a Java deserialization vulnerability in Zoho ManageEngine Pro before 12101 and PAM360 before 5510.

CVSS Score: 9.8

AFFECTED PRODUCTS

- Access Manager Plus version 4302 and below
- Password Manager Pro version 12100 and below
- PAM360 version 5500 and below

To verify if your installation is affected, please take the following steps:

1. Navigate to <PMP/PAM360/AMP_Installation_Directory>/logs
2. Open the access_log_<Date>.txt file
3. Search for the keyword /xmlrpc POST in the text file. If this keyword is not found, your environment is not affected. If it is present, then proceed to the next step.
4. Search for the following line in the logs files. If it is present, then your installation is compromised:
[/xmlrpc-<RandomNumbers>_###_https-jsse-nio2-<YourInstallationPort>-exec-<RandomNumber>] ERROR
org.apache.xmlrpc.server.XmlRpcErrorLogger - InvocationTargetException: java.lang.reflect.InvocationTargetException

REFERENCES

- CISA warns of critical ManageEngine RCE bug used in attacks
- ManageEngine PAM360, Password Manager Pro, and Access Manager Plus remote code execution vulnerability

SECURITY ADVISORY

Date: September 21, 2022

Multiple Vulnerabilities in Microsoft Edge (Chromium based)

BUSINESS IMPACT

Successful exploitation of these vulnerabilities could allow a remote attacker to execute arbitrary code or cause denial of service condition on the targeted system.

RECOMMENDATIONS

1. Update Microsoft Edge (Chromiumbased) to latest version.

INTRODUCTION

Microsoft has released the latest stable update for Microsoft Edge to address multiple vulnerabilities which a remote attacker could exploit to execute arbitrary code or cause a denial of service condition on the targeted system.

The vulnerabilities are tracked as CVE-2022-3195, CVE-2022-3200, CVE-2022-3198, CVE-2022-3197, CVE-2022-3196 and CVE-2022-3199.

These vulnerabilities exist in Microsoft Edge due to Out-of-bounds write error when processing untrusted HTML content in Storage, Heap based buffer overflow issue when processing untrusted HTML content in Internals, Use-after-free errors within the PDF component and Use-after-free error within the Frames component.

AFFECTED PRODUCTS

- Microsoft Edge versions prior to 105.0.1343.42

REFERENCES

- Release notes for Microsoft Edge Security Updates
- Microsoft Edge (Chromium) < 105.0.1343.42 Multiple Vulnerabilities

SECURITY ADVISORY

Date: September 20, 2022

American Airlines has suffered a data breach after falling victim to a phishing scam

RECOMMENDATIONS

1. Ensure all operating systems and software are up to date. Prioritize patching known exploited vulnerabilities.

2. Refrain from opening untrusted links and email attachments without verifying their authenticity.

3. Enable multi-factor authentication if its currently not in use and use secure MFA method, such as a hardware security key or an authentication app.

4. Use solutions that support Fast ID Online (FIDO) v2.0 and certificate-based authentication.

5. Use conditional access policies to prevent from attacks that leverage stolen credentials and session cookie by enabling policies such as compliant devices or trusted IP address requirements.

6. Continuously monitor for suspicious sign-in attempts with suspicious characteristics (for example, location, ISP, user agent, use of anonymizer services).

7. Monitor for unusual mailbox activities such as the creation of Inbox rules with suspicious purposes or unusual amounts of mail item access events by untrusted IP addresses or devices.

8. The airline recommends its customers and employees to enroll to the free complimentary Experian's Credit Monitoring service it is offering to assist them in monitoring credentials and account statements.

9. Stay vigilant on all your account activities. Sign up for SMS and email alerts that can raise red flags in case of suspicious activity.

10. Check the online banking site URL for HTTPS protocol and ensure that the URL is correctly spelled.

11. Control MFA push with features such as number matching to improve user sign-in security. (Ex: Number matching in Azure MFA and number matching in Duo called Duo Verified Push)

12. Configure user email alerts for new MFA and MDM device enrolments. Configure alert on volume of push attempts per account

INCIDENT BRIEFING

American Airlines notified its customers about a security incident on September 16th, 2022. The airline explained, "In July 2022, it has discovered that an unauthorized actor compromised the email accounts of a limited number of American Airlines team members". The company hasn't disclosed the number of affected customers and how many email accounts were breached in the incident.

The threat actors targeted American Airlines team members via phishing attacks and managed to compromise their email accounts successfully. Post-breach, the attackers enumerated sensitive data in the victim's email. Personally Identifiable Information (PII) exposed in the attack include employees' and customers' names, dates of birth, mailing addresses, phone numbers, email addresses, driver's license numbers, passport numbers, and certain medical information.

The threat actors are more likely to leverage the stolen data to conduct financial fraud, identity theft and extortion activities.

LESSON LEARNED

Lack of timely and informed cyber security awareness among employees and management staffs, which allows attackers to take advantage of such gaps in cyber security awareness program, to trick employees and management staffs into installing malicious software and giving out sensitive information via social engineering attack like phishing email, scamming, etc.

REFERENCES

- American Airlines discloses data breach after employee email compromise
- American Airlines Has Been Hacked: Here's What You Should Know

SECURITY ADVISORY

Date: September 13, 2022

High-severity Privilege Escalation bug in pre-installed HP Support Assistant tool

BUSINESS IMPACT

Successful exploitation of the vulnerability could allow a low-privileged attacker to trigger a DLL hijacking flaw to gain elevated privileges on the target system and plant further malware for disruptive operations

RECOMMENDATIONS

Kindly update HP Support Assistant tool

- to the latest version.

INTRODUCTION

HP has released a security advisory to warn users of a newly discovered privilege escalation vulnerability (CVE-2022-38395) in the HP Support Assistant tool that comes pre-installed on all HP laptops and desktop computers.

HP Support Assistant uses HP Performance Tune-up as a diagnostic tool. It uses Fusion to launch HP Performance Tune-up.

The vulnerability exists because the HP Support Assistant application loads DLL libraries in an insecure manner when Fusion launches the HP Performance Tune-up. A local malicious user can place a specially crafted .dll file to trigger a DLL hijacking flaw by launching HP Performance Tune-up from within HP Support Assistant. Successful exploitation enables an attacker to execute malicious DLL with the 'SYSTEM' privileges of the abused HP Support Assistant.

- CVSS Score: 8.2

AFFECTED PRODUCTS

- HP Support Assistant versions earlier than 9.11.
- Fusion versions earlier than 1.38.2601.0.

REFERENCES

- HP fixes severe bug in pre-installed Support Assistant tool

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

19th Sept 2022 – 25th Sept 2022
TRAC-ID: NII22.09.0.4

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	USN-5613-2: Vim regression	• Ubuntu 20.04 LTS	Kindly update to fixed version
Ubuntu Linux	https://ubuntu.com/security/notices/USN-5627-1	• Ubuntu 22.04 LTS • Ubuntu 20.04 LTS	Kindly update to fixed version

REDHAT

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Red Hat Enterprise Linux	RHSA-2022:6716	• Red Hat Enterprise Linux Server for • Power LE - Update Services for SAP • Solutions 8.1 ppc64le • • Red Hat Enterprise Linux for x86_64 - • Update Services for SAP Solutions 8.1 • x86_64	Kindly update to fixed version
Red Hat Enterprise Linux	RHSA-2022:6703	• Red Hat Enterprise Linux Server for • Power LE - Update Services for SAP • Solutions 8.1 ppc64le • • Red Hat Enterprise Linux for x86_64 - • Update Services for SAP Solutions 8.1 • x86_64	Kindly update to fixed version

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

19th Sept 2022 – 25th Sept 2022
TRAC-ID: NII22.09.0.4

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2022-6610	• Oracle Linux 9 (aarch64) • Oracle Linux 9 (x86_64)	Kindly update to fixed version
Oracle Linux	ELSA-2022-6540	• Oracle Linux 8 (aarch64) • Oracle Linux 8 (x86_64)	Kindly update to fixed version

SUSE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
SUSE Linux	SUSE-SU-2022:3425-1	• SUSE-SU-2022:3425-1	Kindly update to fixed version

SECURITY ADVISORY