NETWORK INTELLIGENCE

The Digital Security Company

October 2022, Edition 1.0

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- Thomson Reuters exposed 3TB sensitive customer and corporate database
- Remote code execution bug (CVE-2022-42889) in Apache Commons Text
- Multiple vulnerabilities in Zoom products
- Remote Code Execution, Denial of Service & Memory Leak Vulnerabilities in Adobe Acrobat & Reader

Also Inside

Security Patch Advisory

Critical High Low

Date: October 28, 2022

Thomson Reuters exposed 3TB sensitive customer and corporate database

RECOMMENDATIONS

1. Ensure to have a decent Antivirus program installed on computer.

2. Ensure to be more vigilant while communicating over email or phone call, to eliminate risk of social engineering like phishing.

3. Follow AWS security best practices.

4. Upgrade to the Latest Version of Elasticsearch.

5. Ensure the Elasticsearch is only accessible from OMS, possibly through the use of firewalls.

6. You could add the Elasticsearch Jetty plugin to Elasticsearch nodes to implement authentication and encryption.

7. Elasticsearch uses Lucene internally to index and search data. You should, at a minimum, use file-system permissions to control access to the Lucene files.

8. Plaintext passwords to third-party servers stored in the open database should be hashed with strong algorithms.

9. Ensure that your AWS Elastic Load Balancers (ELBs) listeners are using a secure protocol (HTTPS or SSL).

10.Ensure that your AWS Elastic Load Balancers use access logging to analyze traffic patterns and identify and troubleshoot security issues.

11.Use a Digital Identity Protection tool to scan for leaks of your personal data, notify you instantly of privacy threats and newly discovered breaches, detect social media impersonators.

INCIDENT BRIEFING

Thomson Reuters Corporation is a Canadian multinational media conglomerate. Researchers spotted that Thomson Reuters left three unsecured databases to be publicly accessible.

According to the company, "two of the servers were intended for public use, while the third is a non-production server related to one of Thomson Reuters tools named ONESOURCE Global Trade Product". The tool allows users to "manage export/import, sanction screening, and other trade controls activities and related filings."

Thomson Reuters stated that upon discovering the leaking database, the company immediately took down the open instance and began notifying the affected customers.

The exposed database contained ~3TB of sensitive customer and corporate data, including third-party server passwords in plaintext format. The database has been publicly accessible since October 21 due to a misconfiguration on the AWS Elastic Load Balancing service. The exposed database was already indexed on popular IoT search engines. If the threat actors have accessed the exposed data, it will allow them to gain an initial foothold to the systems used by companies working with Thomson Reuters leading to supply-chain attacks.

Attackers can use the sensitive data to carry out phishing campaigns, impersonate Thomson Reuters and send the company's customers fake invoices, move laterally and pivot through Reuter Thomson's internal systems and launch disruptive ransomware attacks.

AFFECTED PRODUCTS

Misconfiguration issues in software and inadequate security control, often allows attackers to have easy access to sensitive data or gain initial access to cause further damages to cloud-based or on-premises IT Infrastructure.

REFERENCES

- Thomson Reuters collected and leaked at least 3TB of sensitive data

SECURITY ADVISORY

Date: October 19, 2022

Remote code execution bug (CVE-2022-42889) in Apache Commons Text

BUSINESS IMPACT

Successful exploitation of the vulnerability lets attackers run arbitrary commands, trigger internet connections to external servers and services, exfiltrate data and further implant malware for disruptive attacks.

VULNERABILITY DETECTION

Search for files with names that match the pattern commonstext*.jar (the * means “anything can match here”). The suffix .jar is short for java archive, which is how Java libraries are delivered and installed; the prefix commons-text denotes the Apache Common Text software components, and the text in the middle covered by the so-called wildcard * denotes the version number you’ve got

RECOMMENDATIONS

1. Organizations who have direct dependencies on Apache Commons Text should upgrade to the fixed version (1.10.0).

2. Wherever you accept and process untrusted data, especially in Java code, where string interpolation is widely supported and offered as a “feature” in many third-party libraries, make sure you look for and filter out potentially dangerous character sequences from the input first, or take care not to pass that data into string interpolation functions.

INTRODUCTION

Apache Commons Text is a library focused on algorithms working on strings. CVE-2022-42889 (aka Text4Shell) vulnerability exists in Apache Commons Text prior to 1.10.0 that can result in code execution when processing malicious input.

The vulnerability exists due to an insecure interpolation defaults flaw. A remote attacker can send a specially crafted input and execute arbitrary code on the target system.

The vulnerability exists in the StringSubstitutor interpolator object. An interpolator is created by the StringSubstitutor.createInterpolator() method and will allow for string lookups as defined in the StringLookupFactory. This can be used by passing a string “${prefix:name}” where the prefix is the aforementioned lookup. Using the “script”, “dns”, or “url” lookups would allow a crafted string to execute arbitrary scripts when passed to the interpolator object.

- CVSS Score: 9.8

AFFECTED PRODUCTS

- Apache Commons Text versions 1.5 through 1.9

REFERENCES

1. Dangerous hole in Apache Commons Text – like Log4Shell all over again
2. CVE-2022-42889: Apache Commons Text prior to 1.10.0 allows RCE when applied to untrusted input due to insecure interpolation defaults

SECURITY ADVISORY

Date: October 14, 2022

Multiple vulnerabilities in Zoom products

BUSINESS IMPACT

Successful exploitation of these vulnerabilities could allow an authenticated user to bypass security restrictions and perform a denial of service attack on the targeted system.

RECOMMENDATIONS

1. For Zoom On-Premise Deployments, IT administrators can keep their Zoom software up-to-date by following this: https://support.zoom.us/hc/enus/articles/360043960031
2. Ensure to update Zoom software to latest version on desktops. To update Zoom on Windows, macOS, or Linux, sign in to Zoom desktop client > Click your profile picture > Check for Updates. If there is a newer version, Zoom will download and install it.
3. It is recommended to keep Zoom mobile app updated with the latest version via Google Play Store, just to be on the safe side.

INTRODUCTION

Zoom has released fixes to its Zoom products to address two security issues, which could allow an authenticated attacker to bypass security restrictions and cause a denial of service on the targeted system.

Debugging port misconfiguration issue (CVE-2022-28762) exists in Zoom Apps in the Zoom Client for Meetings for macOS. When camera mode rendering context is enabled as part of the Zoom App Layers API by running certain Zoom Apps, the Zoom client opens a local debugging port. A local malicious user could use this debugging port to connect to and control the Zoom Apps running in the Zoom client.

CVSS Score: 7.3

An Improper Access Control flaw (CVE-2022-28761) exists in the Zoom OnPremise Meeting Connector MMR before version 4.8.20220916.131. An attacker authorized to join a meeting or webinar could exploit the vulnerability to prevent participants from receiving audio and video, causing meeting disruptions.

CVSS Score: 6.5

AFFECTED PRODUCTS

- Zoom On-Premise Meeting Connector MMR before version 4.8.20220916.131
- Zoom Client for Meetings for macOS (Standard and for IT Admin) starting with 5.10.6 and prior to 5.12.0

REFERENCES

- Security Bulletin - Zoom
- Denial of service in Zoom On-Premise Meeting Connector MMR

SECURITY ADVISORY

Date: October 14, 2022

Remote Code Execution, Denial of Service & Memory Leak Vulnerabilities in Adobe Acrobat & Reader

BUSINESS IMPACT

Successful exploitation of these vulnerabilities could allow the attacker to obtain sensitive information, execute arbitrary code and cause denial of service on the targeted system.

RECOMMENDATIONS

Ensure Adobe Acrobat and Reader for Windows and macOS is updated with latest security patches.

The latest product versions are available to end users via one of the following methods:
• Users can update their product installations manually by choosing Help > Check for Updates. • The products will update automatically, without requiring user intervention, when updates are detected. • The full Acrobat Reader installer can be downloaded from the Acrobat Reader Download Center.

For IT administrators (managed environments):
• Refer to the specific release note version for links to installers.
• Install updates via your preferred methodology, such as AIP-GPO, bootstrapper, SCUP/SCCM (Windows), or on macOS, Apple Remote Desktop and SSH.

INTRODUCTION

Adobe has released security updates to address multiple Critical and High Severity vulnerabilities in Adobe Acrobat and Reader for Windows and macOS.

The vulnerabilities are tracked as CVE-2022-35691, CVE-2022-38437, CVE2022-38450, CVE-2022-42339, CVE-2022-38449 and CVE-2022-42342.

These vulnerabilities exist in Adobe Acrobat and Acrobat Reader due to Use after Free, NULL Pointer Dereference, Stack-based Buffer Overflow and Outof-bounds Read errors. A remote attacker could exploit these vulnerabilities by sending a specially crafted PDF file to the targeted system and convincing the user to open a crafted document.

AFFECTED PRODUCTS

- Acrobat DC and Acrobat Reader DC (Continuous) versions 22.002.20212 and earlier for Windows & MacOS.
- Acrobat 2020 and Acrobat Reader 2020 (Classic 2020) versions 20.005.30381 and earlier for Windows & MacOS.

REFERENCES

- Security update available for Adobe Acrobat and Reader | APSB22-46

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

10th Oct 2022 – 16th Oct 2022
TRAC-ID: NII22.10.0.3

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	USN-5666-1: OpenSSH vulnerability	• Ubuntu 16.04 ESM	Kindly update to fixed version
Ubuntu Linux	USN-5665-1: PCRE vulnerabilities	• Ubuntu 16.04 ESM	Kindly update to fixed version

SUSE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
SUSE Linux	SUSE-SU2022:3584-1	• SUSE Linux Enterprise Server 12-SP5	Kindly update to fixed version
SUSE Linux	SUSE-SU2022:3583-1	• SUSE OpenStack Cloud 9 • SUSE OpenStack Cloud Crowbar 9	Kindly update to fixed version

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

10th Oct 2022 – 16th Oct 2022
TRAC-ID: NII22.10.0.3

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2022-6913	• Oracle Linux 9 (aarch64) • Oracle Linux 9 (x86_64)	Kindly update to fixed version
Oracle Linux	ELSA-2022-6911	• Oracle Linux 8 (aarch64) • Oracle Linux 8 (x86_64)	Kindly update to fixed version

SONICWALL

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
SonicWall GMS	GMS FILE PATH MANIPULATION	• SonicWall GMS versions prior 9.3.2.	Kindly update to fixed version

SECURITY ADVISORY