This Month In

VULNERABILITIES & PATCHES

Qualys® Research

#PatchWithQualys

Bharat Jogi | Eran Livne

Today's Agenda

Monthly overview of Qualys vulnerability and patch coverage

Recent, noteworthy vulnerabilities & Qualys' coverage

- Multiple Log4j Vulnerabilities (CVE-2021-44228, CVE-2021-45046,CVE-2021-45105,CVE-2021-44832)
- Microsoft Hyper Text Transfer Protocol RCE Vulnerability (CVE-2022-21907)
- Windows IKE Extension Vulnerabilities (CVE-2022-21829)
- Microsoft Sharepoint Exchange Server Code Execution Vulnerability (CVE-2022-21837)

Leveraging Qualys integrated PM

- Automated Qualys Patch Management
- Proactive Zero-Touch Patch

Vulnerability & Patch Coverage Overview

Dec 2021– Jan 2022

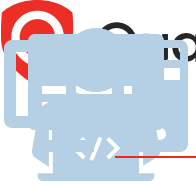
Qualys Released

1241	QIDs Released
2816	Unique CVEs
1280	Patch Links

QID Severity Distribution	
Severity	**QIDs**
Critical	**183**
High	**435**
Medium	537
Low	84
Informational	2

Recent, noteworthy CVEs & QID coverage

CVEs	QID	Vendor / Product / Advisory	Vuln Type	Exploit Available
CVE-2021-44228, CVE-2021-44832, CVE-2021-45105 and CVE-2021-45046	730297,376157, 376160,...	Log4j Multiple Vulnerabilities	Remote Code Execution	Yes
CVE-2022-21907	91852	Microsoft Hyper Text Transfer Protocol RCE Vulnerability	Remote Code Execution	No
CVE-2022-21829	376232	Windows IKE Extension Vulnerabilities	Remote Code Execution	No
CVE-2022-21837	110339	Microsoft Sharepoint Exchange Server Code Execution Vulnerability	Remote Code Execution	No



What is Log4j?

Log4j2 is a ubiquitous library used by millions of Java applications.

It is one of the most common libraries used for Logging by Java applications

The jar file for Log4j can be copied/bundled anywhere on the file system

Log4Shell Vulnerability Detail

- This vulnerability allows an attacker to execute arbitrary code on a remote system (RCE)
- This vulnerability is easy to exploit, but not trivial to detect
  - It is not known which parameters are logged by the application ahead of time.
  - Log4j can be present at any location on the file system

Log4j Coverage

Qualys Released

4	Unique CVEs
92	QIDs Released
81	Authenticated QIDs
11	Un-Authenticated QIDs
5	Scan Utility Based QIDs

Qualys Coverage

QID 730297 Apache Log4j Remote Code Execution (RCE) Vulnerability

- QID attempts to exploit common parameters that are logged by Java applications using Log4j and waits for callback response to the scanner.

QID 376157 Apache Log4j Remote Code Execution (RCE) Vulnerability

- QID leverages the OS package manager to identify vulnerable Log4j packages
- Attempts to find vulnerable locations via locate command
- Identify running processes using Log4j via ls proc

QID 376160 Apache Log4j RCE via Qualys Log4j Scan Utility

- QID leverages the external Qualys log4j Scan utility to scan the entire file system to identify all vulnerable log4j installations on a host

Updates to Scan Utility

- The Scan Utility now supports Linux, Windows and Unix-based OS like AIX, Solaris and MacOS
- The Windows scan utility now also support remediation action

Qualys Coverage (WAS)

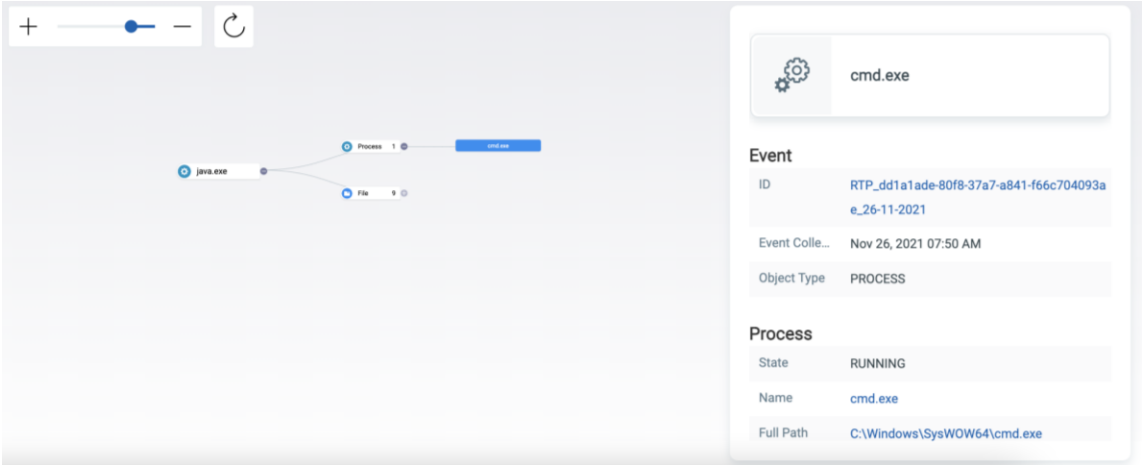
150440 Apache Log4j Remote Code Execution (RCE) Vulnerability (Log4Shell)

- The Web Application Security (WAS) module uses our Out Of Band detection mechanism to inject payloads into HTTP headers

Qualys Coverage (EDR)

Detect and Respond to Endpoint Malware and Attacks Exploiting Log4J

- Detect java.exe processes with a LDAP Network connection
- Search for Log4J Vulnerabilities by collecting and inventorying all .jar files on a system
- Detect internal lateral movement attempts by flagging on curl.exe and Log4J payloads
- Detect java.exe process that spawn unusual child processes:
  - cmd.exe
  - pwsh.exe
  - powershell.exe
  - perl.exe
  - Python.exe
  - ruby.exe
  - wget.exe
  - curl.exe



Qualys

SEVERITY
4

Microsoft Hyper Text Transfer Protocol RCE Vulnerability

CVEs: CVE-2022-21907

QID	Vendor Security Advisory	Vuln Type	Exploit Available
91852	Multiple KBs	Code Execution	No

CVE-2022-21907
This vulnerability has a CVSSv3.1 score of 9.8/10. This vulnerability affects Windows Servers configured as a webserver. To exploit this vulnerability an unauthenticated attacker could send a specially crafted packet to a vulnerable server utilizing the HTTP Protocol Stack to process packets. This vulnerability is known to be wormable. Exploitability Assessment: *Exploitation More Likely*.

Qualys

SEVERITY
5

Windows IKE Extension RCE Vulnerability

CVEs: CVE-2022-21829

QID	Vendor Security Advisory	Vuln Type	Exploit Available
376232	Multiple KBs	Code Execution	No

CVE-2022-21829
This vulnerability has a CVSSv3.1 score of **9.8**/10. This vulnerability affects systems with Internet Key Exchange (IKE) version 2. While at this time the details of this vulnerability are limited, a remote attacker could trigger multiple vulnerabilities when the IPSec service is running on the Windows system without being authenticated. Exploitability Assessment: *Exploitation Less Likely*.

Qualys.

SEVERITY
5

Microsoft Sharepoint Exchange Server Code Execution Vulnerability

CVEs: CVE-2022-21837

QID	Vendor Security Advisory	Vuln Type	Exploit Available
110339	Multiple KBs	Code Execution	No

CVE-2022-21837
This vulnerability has a CVSSv3.1 score of **8.3**/10. An attacker can use this vulnerability to gain access to the domain and could perform remote code execution on the SharePoint server to elevate themselves to SharePoint admin. Assessment: *Exploitation Less Likely*.

Qualys
Patch Management

FREE 60-DAY
Patch Management Trial
qualys.com/ forms/patch-management/

Qualys.

Q&A