Network Vulnerability Scanner Report

✔ eternalspring.pentest-ground.com

Summary

Overall risk level:

High

Risk ratings:

Scan information:

Start time:	2022-05-25 12:22:33 UTC+03
Finish time:	2022-05-25 12:24:16 UTC+03
Scan duration:	1 min, 43 sec
Tests performed:	15/15
Scan status:	Finished

Findings

EternalBlue - Remote Code Execution (CVE-2017-0144)

Port:445
We managed to detect that Windows 10 Pro 14393 located at eternalspring.pentest-ground.com:445 is vulnerable.
The vulnerability was detected by sending 4 payloads through the SMB protocol and looking for the STATUS_INSUFF_SERVER_RESOURCES error code in the final response.

Details

Vulnerability description:
We found that the target server is vulnerable to CVE-2017-0144, a Remote Code Execution in Microsoft Windows affecting the SMBv1 protocol. The root cause of this vulnerability is the improper packet handling of the SMBv1 traffic.
We have detected this vulnerability by looking for the **STATUS_INSUFF_SERVER_RESOURCES** error code in the server response after sending the payloads via the SMBv1 protocol.

Risk description:
The risk exists that a remote unauthenticated attacker could execute arbitrary code via specially crafted SMBv1 requests and thus can compromise the target system.

Recommendation:
We recommend enabling the Windows Updates which will install the latest patches for your Windows version that will solve the issue.

References:
https://nvd.nist.gov/vuln/detail/cve-2017-0144
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0144

Spring Core - Remote Code Execution (Spring4Shell - CVE-2022-22965)

Port:8080
We managed to find a Remote Code Execution vulnerability in Spring Core, by sending the following payload (**whoami** command):

HTTP Request:
POST /helloworld/greeting HTTP/1.1
Host: eternalspring.pentest-ground.com

class.module.classLoader.resources.context.parent.pipeline.first.pattern=%25%7Bp...
HTTP Response:
HTTP 200 OK

HTTP Request:
GET /obvxvacfmf.jsp?cmd=whoami HTTP/1.1
Host: eternalspring.pentest-ground.com
HTTP Response:
HTTP 200 OK

nt authority\local service

Details

Vulnerability description:
We found that the target server is vulnerable to CVE-2022-22965, a Remote Code Execution in Spring Core Framework affecting the web application deployed as a WAR. The root cause of this vulnerability is the insecure access to ClassLoader in Java 9+ which is used in Spring Framework and can be used for uploading a malicious webshell. Spring Framework is affected in versions below 5.2.20 or in version 5.3.18 and Spring Boot is affected in versions lower than 2.6.6.
We have detected this vulnerability by sending a chain of HTTP POST requests with modified classLoader parameters to the vulnerable aplication in order to upload a webshell and by using a HTTP GET request to check the output of the `id` command.

Risk description:
The risk exists that a remote unauthenticated attacker can fully compromise the server in order to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:
We recommend upgrading the Spring Framwork or Spring Boot to the newest version and check the newest Java security fix for versions higher or equal with 9

References:
https://jfrog.com/blog/springshell-zero-day-vulnerability-all-you-need-to-know
https://www.lunasec.io/docs/blog/spring-rce-vulnerabilities/
https://nvd.nist.gov/vuln/detail/CVE-2022-22965

Scan coverage information

Port	State	Service	Product	Product Version
445	open	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds	
8080	open	http	Apache Tomcat	9.0.60

Details

Risk description:
This is the list of ports that have been found open on the target hosts. Having unnecessary open ports may expose the target systems to more risks because those network services and applications may contain vulnerabilities.

Recommendation:
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

Not vulnerable to Apache Struts 2 - Remote Code Execution (CVE-2018-11776) (port 8080)

Not vulnerable to VMware vCenter - Remote Code Execution (Log4Shell - CVE-2021-44228) (port 8080)

Not vulnerable to ManageEngine ADSelfService Plus - Unauthenticated Remote Code Execution (CVE-2021-40539) (port 8080)

Not vulnerable to Log4j - Remote Code Execution (Log4Shell - CVE-2021-45046) (port 8080)

Not vulnerable to Spring Cloud Function - Remote Code Execution (CVE-2022-22963) (port 8080)

Not vulnerable to VMware Workspace One - Remote Code Execution (CVE-2022-22954) (port 8080)

Not vulnerable to Node.js Systeminformation - Command Injection (CVE-2021-21315) (port 8080)

Not vulnerable to Log4j - Remote Code Execution (Log4Shell - CVE-2021-44228) (port 8080)

Not vulnerable to Apache Struts - Remote Code Execution (Log4Shell - CVE-2021-44228) (port 8080)

Not vulnerable to ManageEngine Desktop Central - Authentication Bypass and Remote Code Execution (CVE-2021-44515) (port 8080)

Not vulnerable to Apache OFBiz - Remote Code Execution (CVE-2021-26295) (port 8080)

Not vulnerable to Apache Tomcat - Remote Code Execution (Log4Shell - CVE-2021-44228) (port 8080)

Scan coverage information

List of tests performed (15/15)

- Checking for open ports...
- Checking for Microsoft Eternalblue - MS17_010 (CVE-2017-0144)... (Sniper module)
- Checking for Apache Struts 2 - Remote Code Execution (CVE-2018-11776)... (Sniper module)
- Checking for VMware vCenter - Remote Code Execution (Log4Shell - CVE-2021-44228)... (Sniper module)
- Checking for Spring Core - Remote Code Execution (Spring4Shell - CVE-2022-22965)... (Sniper module)
- Checking for ManageEngine ADSelfService Plus - Unauthenticated Remote Code Execution (CVE-2021-40539)... (Sniper module)
- Checking for Log4j - Remote Code Execution (Log4Shell - CVE-2021-45046)... (Sniper module)

- Checking for Spring Cloud Function - Remote Code Execution (CVE-2022-22963)... (Sniper module)
- Checking for VMware Workspace One - Remote Code Execution (CVE-2022-22954)... (Sniper module)
- Checking for Node.js Systeminformation - Command Injection (CVE-2021-21315)... (Sniper module)
- Checking for Log4j - Remote Code Execution (Log4Shell - CVE-2021-44228)... (Sniper module)
- Checking for Apache Struts - Remote Code Execution (Log4Shell - CVE-2021-44228)... (Sniper module)
- Checking for ManageEngine Desktop Central - Authentication Bypass and Remote Code Execution (CVE-2021-44515)... (Sniper module)
- Checking for Apache OFBiz - Remote Code Execution (CVE-2021-26295)... (Sniper module)
- Checking for Apache Tomcat - Remote Code Execution (Log4Shell - CVE-2021-44228)... (Sniper module)

Scan parameters

Target:	eternalspring.pentest-ground.com
Scan type:	Sniper
Check alive:	True
Protocol type:	Tcp
Ports to scan:	445,8080