

# Docker Test Report

12 targets scanned | 26 findings

Report generated: February 12, 2026

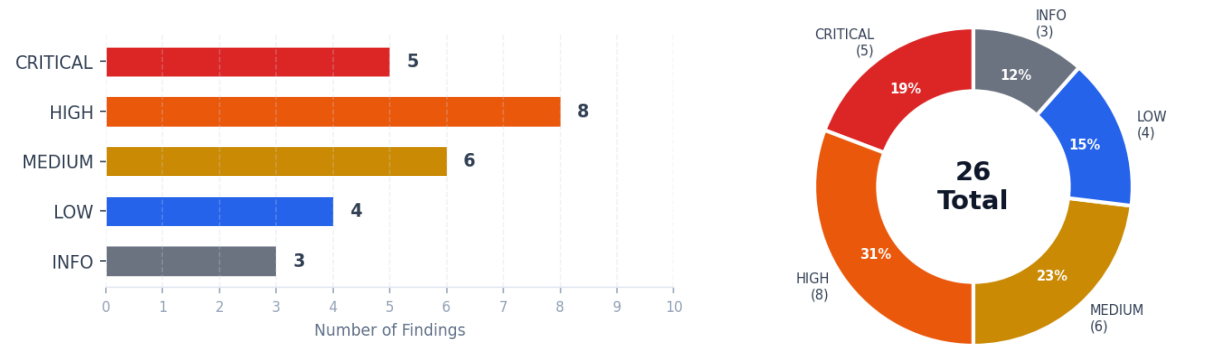
Scan period: 2025-02-10T14:32:07

5 CRITICAL | 8 HIGH | 6 MEDIUM | 4 LOW | 3  
INFO

Generated by **NucleiReport** | Nuclei Vulnerability Scanner

## Executive Summary

This assessment identified **26 findings** across 12 targets. **5 critical** and **8 high** severity issues require immediate attention.



## Findings by Severity

Severity	Count	Percentage
CRITICAL	5	19.2%
HIGH	8	30.8%
MEDIUM	6	23.1%
LOW	4	15.4%
INFO	3	11.5%
TOTAL	26	100.0%

## Top Critical Findings

- [CRITICAL]** Apache Log4j RCE (Log4Shell) (CVSS 10.0) - <https://acme-corp.com>
- [CRITICAL]** Palo Alto PAN-OS Command Injection (CVSS 10.0) - <https://acme-corp.com>
- [CRITICAL]** Atlassian Confluence Broken Access Control (CVSS 9.8) - <https://wiki.acme-corp.com>
- [CRITICAL]** Fortinet FortiOS Out-of-Bound Write (CVSS 9.8) - <https://vpn.acme-corp.com>
- [CRITICAL]** HTTP/2 Rapid Reset Attack (CVSS 7.5) - <https://acme-corp.com>

# Detailed Findings

## CRITICAL - 5 findings

### [CRITICAL] Apache Log4j RCE (Log4Shell) | CVE-2021-44228 | CVSS: 10.0

Template: CVE-2021-44228

Apache Log4j2 <=2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints.

**Target:** https://acme-corp.com

**Matched At:** https://acme-corp.com/api/v2/login

**IP:** 203.0.113.10

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

**Remediation:** Upgrade to Log4j 2.17.1 or later. Remove JndiLookup class from classpath as a temporary mitigation.

#### References:

- <https://nvd.nist.gov/vuln/detail/CVE-2021-44228>
- <https://logging.apache.org/log4j/2.x/security.html>

### [CRITICAL] Palo Alto PAN-OS Command Injection | CVE-2024-3400 | CVSS: 10.0

Template: CVE-2024-3400

A command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS allows an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

**Target:** https://acme-corp.com

**Matched At:** https://acme-corp.com:443/ssl-vpn/login

**IP:** 203.0.113.10

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

**Remediation:** Apply PAN-OS hotfix. Enable Threat Prevention signatures as interim mitigation.

#### References:

- <https://nvd.nist.gov/vuln/detail/CVE-2024-3400>
- <https://security.paloaltonetworks.com/CVE-2024-3400>

## **[CRITICAL] Atlassian Confluence Broken Access Control | CVE-2023-22515 | CVSS: 9.8**

Template: CVE-2023-22515

Atlassian Confluence Data Center and Server is vulnerable to a broken access control vulnerability that allows an external attacker to create unauthorized Confluence administrator accounts and access Confluence instances.

**Target:** <https://wiki.acme-corp.com>

**Matched At:** <https://wiki.acme-corp.com/server-info.action>

**IP:** 203.0.113.20

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Remediation:** Upgrade Confluence to patched versions 8.3.3, 8.4.3, or 8.5.2+.

### References:

- <https://nvd.nist.gov/vuln/detail/CVE-2023-22515>
- <https://confluence.atlassian.com/security/cve-2023-22515-broken-access-control-vulnerability-in-confluence-data-center-and-server-1295682276.html>

## **[CRITICAL] Fortinet FortiOS Out-of-Bound Write | CVE-2024-21762 | CVSS: 9.8**

Template: CVE-2024-21762

A out-of-bounds write vulnerability in Fortinet FortiOS allows a remote unauthenticated attacker to execute arbitrary code or command via specially crafted HTTP requests.

**Target:** <https://vpn.acme-corp.com>

**Matched At:** <https://vpn.acme-corp.com/remote/logincheck>

**IP:** 203.0.113.30

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Remediation:** Upgrade FortiOS to the latest patched version. Disable SSL VPN as a workaround.

### References:

- <https://nvd.nist.gov/vuln/detail/CVE-2024-21762>
- <https://www.fortiguard.com/psirt/FG-IR-24-015>

## **[CRITICAL] HTTP/2 Rapid Reset Attack | CVE-2023-44487 | CVSS: 7.5**

Template: CVE-2023-44487

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

**Target:** https://acme-corp.com

**Matched At:** https://acme-corp.com/

**IP:** 203.0.113.10

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**Remediation:** Update web server and load balancer software to patched versions.  
Implement rate limiting on HTTP/2 stream resets.

### **References:**

- <https://nvd.nist.gov/vuln/detail/CVE-2023-44487>
- <https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-vulnerability-cve-2023-44487>

# Detailed Findings (continued)

## HIGH - 8 findings

### [HIGH] F5 BIG-IP Authentication Bypass | CVE-2023-46747 | CVSS: 9.8

Template: CVE-2023-46747

Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands.

**Target:** https://lb.acme-corp.com

**Matched At:** https://lb.acme-corp.com/tmui/login.jsp

**IP:** 203.0.113.40

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Remediation:** Apply the F5 hotfix or upgrade to a patched BIG-IP version.

#### References:

- <https://nvd.nist.gov/vuln/detail/CVE-2023-46747>
- <https://my.f5.com/manage/s/article/K000137353>

### [HIGH] MOVEit Transfer SQL Injection | CVE-2023-34362 | CVSS: 9.8

Template: CVE-2023-34362

Progress MOVEit Transfer contains a SQL injection vulnerability that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database and execute arbitrary code.

**Target:** https://files.acme-corp.com

**Matched At:** https://files.acme-corp.com/moveitisapi/moveitisapi.dll

**IP:** 203.0.113.50

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Remediation:** Apply MOVEit Transfer patch immediately. Block external HTTP/HTTPS traffic to the MOVEit Transfer environment.

#### References:

- <https://nvd.nist.gov/vuln/detail/CVE-2023-34362>
- <https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023>

## **[HIGH]** Cisco IOS XE Web UI Privilege Escalation | CVE-2023-20198 | CVSS: 9.8

Template: CVE-2023-20198

Cisco IOS XE Software Web UI contains a privilege escalation vulnerability that allows a remote unauthenticated attacker to create an account with privilege level 15 access.

**Target:** https://router.acme-corp.com

**Matched At:** https://router.acme-corp.com/webui

**IP:** 203.0.113.1

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Remediation:** Disable the HTTP Server feature on internet-facing systems. Apply Cisco patches when available.

### References:

- <https://nvd.nist.gov/vuln/detail/CVE-2023-20198>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z>

## **[HIGH]** Spring4Shell - Spring Framework RCE | CVE-2022-22965 | CVSS: 9.8

Template: CVE-2022-22965

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution via data binding.

**Target:** https://app.acme-corp.com

**Matched At:** https://app.acme-corp.com/spring/login

**IP:** 203.0.113.60

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Remediation:** Upgrade Spring Framework to 5.3.18+ or 5.2.20+. Upgrade to JDK patched versions.

### References:

- <https://nvd.nist.gov/vuln/detail/CVE-2022-22965>
- <https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement>

## **[HIGH] Microsoft Exchange Server SSRF (ProxyLogon) | CVE-2021-26855 | CVSS: 9.8**

Template: CVE-2021-26855

Microsoft Exchange Server contains a server-side request forgery vulnerability that allows an attacker to send arbitrary HTTP requests and authenticate as the Exchange server.

**Target:** https://mail.acme-corp.com

**Matched At:** https://mail.acme-corp.com/owa/auth/logon.aspx

**IP:** 203.0.113.70

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Remediation:** Apply Microsoft Exchange cumulative updates and security patches immediately.

### References:

- <https://nvd.nist.gov/vuln/detail/CVE-2021-26855>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855>

## **[HIGH] JetBrains TeamCity Authentication Bypass | CVE-2023-42793 | CVSS: 9.8**

Template: CVE-2023-42793

In JetBrains TeamCity before 2023.05.4, authentication bypass allowing to perform admin actions was possible.

**Target:** https://ci.acme-corp.com

**Matched At:** https://ci.acme-corp.com/app/rest/users/id:1/tokens/RPC2

**IP:** 203.0.113.80

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Remediation:** Upgrade TeamCity to version 2023.05.4 or later.

### References:

- <https://nvd.nist.gov/vuln/detail/CVE-2023-42793>
- <https://blog.jetbrains.com/teamcity/2023/09/critical-security-issue-affecting-teamcity-on-premises/>

## **[HIGH] F5 BIG-IP iControl REST Authentication Bypass | CVE-2022-1388 | CVSS: 9.8**

Template: CVE-2022-1388

F5 BIG-IP iControl REST has an authentication bypass vulnerability which may allow an unauthenticated attacker with network access to execute arbitrary system commands.

**Target:** https://lb.acme-corp.com

**Matched At:** https://lb.acme-corp.com/mgmt/tm/util/bash

**IP:** 203.0.113.40

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Remediation:** Update BIG-IP to a patched version. Restrict access to the iControl REST API.

### **References:**

- <https://nvd.nist.gov/vuln/detail/CVE-2022-1388>
- <https://support.f5.com/csp/article/K23605346>

## **[HIGH] Microsoft SharePoint Server Privilege Escalation | CVE-2023-29357 | CVSS: 9.1**

Template: CVE-2023-29357

Microsoft SharePoint Server contains a privilege escalation vulnerability that allows an attacker who has gained access to spoofed JWT authentication tokens to use them to execute a network attack which bypasses authentication.

**Target:** https://sharepoint.acme-corp.com

**Matched At:** https://sharepoint.acme-corp.com/\_api/web/siteusers

**IP:** 203.0.113.90

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

**Remediation:** Apply Microsoft SharePoint security updates.

### **References:**

- <https://nvd.nist.gov/vuln/detail/CVE-2023-29357>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29357>

# Detailed Findings (continued)

## MEDIUM - 6 findings

### [MEDIUM] Microsoft Outlook Privilege Escalation | CVE-2023-23397 | CVSS: 7.5

Template: CVE-2023-23397

Microsoft Outlook contains a privilege escalation vulnerability that allows an attacker to access a user's Net-NTLMv2 hash via a crafted email.

**Target:** https://mail.acme-corp.com

**Matched At:** https://mail.acme-corp.com/owa/

**IP:** 203.0.113.70

**CVSS Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**Remediation:** Apply Microsoft security updates. Block outbound SMB traffic (TCP port 445).

#### References:

- <https://nvd.nist.gov/vuln/detail/CVE-2023-23397>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397>

### [MEDIUM] Expired SSL Certificate | CVSS: 5.3

Template: ssl-expired-cert

The SSL/TLS certificate for this host has expired, which can lead to man-in-the-middle attacks and loss of user trust.

**Target:** https://staging.acme-corp.com

**Matched At:** https://staging.acme-corp.com:443

**IP:** 203.0.113.100

**Remediation:** Renew the SSL/TLS certificate and configure automatic renewal.

#### References:

- [https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\\_Application\\_Security\\_Testing/09-Testing\\_for\\_Weak\\_Cryptography/01-Testing\\_for\\_Weak\\_Transport\\_Layer\\_Security](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/01-Testing_for_Weak_Transport_Layer_Security)

## **[MEDIUM] CORS Misconfiguration | CVSS: 5.3**

Template: cors-misconfig

Cross-Origin Resource Sharing is misconfigured, allowing any origin to access resources. This can lead to data theft via cross-site requests.

**Target:** https://api.acme-corp.com

**Matched At:** https://api.acme-corp.com/v1/users

**IP:** 203.0.113.11

**Remediation:** Configure CORS to only allow trusted origins. Avoid using wildcard (\*) in Access-Control-Allow-Origin.

### References:

- [https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\\_Application\\_Security\\_Testing/11-Client-side\\_Testing/07-Testing\\_Cross-Origin\\_Resource\\_Sharing](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/11-Client-side_Testing/07-Testing_Cross-Origin_Resource_Sharing)

## **[MEDIUM] Content-Security-Policy Header Missing | CVSS: 5.0**

Template: csp-header-missing

The Content-Security-Policy header is missing, which increases the risk of cross-site scripting (XSS) and data injection attacks.

**Target:** https://acme-corp.com

**Matched At:** https://acme-corp.com/

**IP:** 203.0.113.10

**Remediation:** Implement a Content-Security-Policy header with appropriate directives.

### References:

- <https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>  
- <https://owasp.org/www-project-secure-headers/>

## **[MEDIUM] Open Redirect Detected | CVSS: 4.7**

Template: open-redirect

An open redirect vulnerability was detected that could be used in phishing campaigns to redirect users to malicious sites.

**Target:** https://acme-corp.com

**Matched At:** https://acme-corp.com/login?redirect=https://evil.com

**IP:** 203.0.113.10

**Remediation:** Validate and whitelist redirect URLs. Do not pass user-controlled URLs directly to redirect functions.

### References:

- <https://cwe.mitre.org/data/definitions/601.html>
- [https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\\_Application\\_Security\\_Testing/11-Client-side\\_Testing/04-Testing\\_for\\_Client-side\\_URL\\_Redirect](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/11-Client-side_Testing/04-Testing_for_Client-side_URL_Redirect)

## **[MEDIUM] X-Frame-Options Header Missing | CVSS: 4.3**

Template: x-frame-options-missing

The X-Frame-Options HTTP header is missing, which means the site could be vulnerable to clickjacking attacks.

**Target:** https://acme-corp.com

**Matched At:** https://acme-corp.com/

**IP:** 203.0.113.10

**Remediation:** Add X-Frame-Options header with DENY or SAMEORIGIN directive.

### References:

- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>
- <https://owasp.org/www-project-web-security-testing-guide/>

# Detailed Findings (continued)

## LOW - 4 findings

### [LOW] Directory Listing Enabled | CVSS: 3.7

Template: directory-listing

Directory listing is enabled on the web server, which could expose sensitive files and internal structure information to attackers.

**Target:** https://acme-corp.com

**Matched At:** https://acme-corp.com/assets/

**IP:** 203.0.113.10

**Remediation:** Disable directory listing in web server configuration. Add index files to directories.

#### References:

- [https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\\_Application\\_Security\\_Testing/02-Configuration\\_and\\_Deployment\\_Management\\_Testing/04-Review\\_Old\\_Backup\\_and\\_Unreferenced\\_Files\\_for\\_Sensitive\\_Information](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/04-Review_Old_Backup_and_Unreferenced_Files_for_Sensitive_Information)

### [LOW] Strict-Transport-Security Header Missing | CVSS: 3.1

Template: missing-hsts

The HTTP Strict-Transport-Security header is not set, which means browsers will not enforce HTTPS connections, leaving users vulnerable to SSL stripping attacks.

**Target:** https://acme-corp.com

**Matched At:** https://acme-corp.com/

**IP:** 203.0.113.10

**Remediation:** Add Strict-Transport-Security header with appropriate max-age value.

#### References:

- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>  
- <https://owasp.org/www-project-secure-headers/>

### [LOW] Cookie Without HttpOnly Flag | CVSS: 3.1

Template: cookie-no-httponly

A session cookie is set without the HttpOnly flag, making it accessible to JavaScript and increasing the risk of cookie theft through XSS attacks.

**Target:** https://app.acme-corp.com

**Matched At:** https://app.acme-corp.com/login

**IP:** 203.0.113.60

**Remediation:** Set the HttpOnly flag on all sensitive cookies.

#### References:

- <https://owasp.org/www-community/HttpOnly>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>

### [LOW] Cookie Without Secure Flag | CVSS: 2.6

Template: cookie-no-secure

A cookie is set without the Secure flag, meaning it could be transmitted over unencrypted HTTP connections.

**Target:** https://app.acme-corp.com

**Matched At:** https://app.acme-corp.com/login

**IP:** 203.0.113.60

**Remediation:** Set the Secure flag on all cookies to ensure they are only sent over HTTPS.

#### References:

- [https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\\_Application\\_Security\\_Testing/06-Session\\_Management\\_Testing/02-Testing\\_for\\_Cookies\\_Attributes](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes)

# Detailed Findings (continued)

## INFO - 3 findings

### [INFO] robots.txt Exposed

Template: robots-txt

The robots.txt file is publicly accessible and may reveal hidden paths or administrative endpoints.

**Target:** https://acme-corp.com

**Matched At:** https://acme-corp.com/robots.txt

**IP:** 203.0.113.10

**Remediation:** Review robots.txt for sensitive path disclosures. This is informational only.

#### References:

- <https://developers.google.com/search/docs/crawling-indexing/robots/intro>

### [INFO] WAF Detected - Cloudflare

Template: waf-detect

A Web Application Firewall (Cloudflare) was detected protecting the target application.

**Target:** https://acme-corp.com

**Matched At:** https://acme-corp.com/

**IP:** 203.0.113.10

**Remediation:** Informational finding. No action required.

#### References:

- <https://www.cloudflare.com/waf/>

## [INFO] Nginx Version Detected

Template: tech-detect-nginx

The target is running Nginx web server. The version was detected from server response headers.

**Target:** https://api.acme-corp.com

**Matched At:** https://api.acme-corp.com/

**IP:** 203.0.113.11

**Remediation:** Consider removing or obfuscating server version headers to reduce information leakage.

### References:

- <https://nginx.org/>

# Appendices

## A. Targets Scanned

#	Host	Findings
1	https://acme-corp.com	10
2	https://wiki.acme-corp.com	1
3	https://vpn.acme-corp.com	1
4	https://lb.acme-corp.com	2
5	https://files.acme-corp.com	1
6	https://router.acme-corp.com	1
7	https://app.acme-corp.com	3
8	https://mail.acme-corp.com	2
9	https://ci.acme-corp.com	1
10	https://sharepoint.acme-corp.com	1
11	https://staging.acme-corp.com	1
12	https://api.acme-corp.com	2

## B. Scan Metadata

Total Findings	26
Unique Targets	12
Report Generated	2026-02-12 05:36:46
Scan Start	2025-02-10T14:32:07
Scan End	2025-02-10T14:37:50
Critical Findings	5
High Findings	8
Medium Findings	6
Low Findings	4
Info Findings	3

## C. Severity Definitions

Severity	CVSS Range	Description
<b>CRITICAL</b>	9.0 - 10.0	Exploitation is straightforward and usually results in system-level compromise. Immediate remediation is required.
<b>HIGH</b>	7.0 - 8.9	Exploitation is possible with moderate complexity. Could result in significant data loss or system impact.
<b>MEDIUM</b>	4.0 - 6.9	Exploitation requires specific conditions. Impact is limited but could escalate if combined with other vulnerabilities.
<b>LOW</b>	0.1 - 3.9	Exploitation is difficult or impact is minimal. Should be addressed as part of regular maintenance.
<b>INFO</b>	0.0	Informational finding with no direct security impact. Useful for understanding the target's configuration.

## D. Findings Quick Reference

#	Severity	Name	Target	CVSS
1	CRIT	Apache Log4j RCE (Log4Shell)	https://acme-corp.com	10.0
2	CRIT	Palo Alto PAN-OS Command Injection	https://acme-corp.com	10.0
3	CRIT	Atlassian Confluence Broken Acce...	https://wiki.acme-corp.com	9.8
4	CRIT	Fortinet FortiOS Out-of-Bound Write	https://vpn.acme-corp.com	9.8
5	CRIT	HTTP/2 Rapid Reset Attack	https://acme-corp.com	7.5
6	HIGH	F5 BIG-IP Authentication Bypass	https://lb.acme-corp.com	9.8
7	HIGH	MOVEit Transfer SQL Injection	https://files.acme-corp.com	9.8
8	HIGH	Cisco IOS XE Web UI Privilege Es...	https://router.acme-corp.com	9.8
9	HIGH	Spring4Shell - Spring Framework RCE	https://app.acme-corp.com	9.8
10	HIGH	Microsoft Exchange Server SSRF (...)	https://mail.acme-corp.com	9.8
11	HIGH	JetBrains TeamCity Authenticatio...	https://ci.acme-corp.com	9.8
12	HIGH	F5 BIG-IP iControl REST Authenti...	https://lb.acme-corp.com	9.8
13	HIGH	Microsoft SharePoint Server Priv...	https://sharepoint.acme-cor...	9.1
14	MEDI	Microsoft Outlook Privilege Esca...	https://mail.acme-corp.com	7.5
15	MEDI	Expired SSL Certificate	https://staging.acme-corp.com	5.3

#	Severity	Name	Target	CVSS
16	MEDI	CORS Misconfiguration	https://api.acme-corp.com	5.3
17	MEDI	Content-Security-Policy Header M...	https://acme-corp.com	5.0
18	MEDI	Open Redirect Detected	https://acme-corp.com	4.7
19	MEDI	X-Frame-Options Header Missing	https://acme-corp.com	4.3
20	LOW	Directory Listing Enabled	https://acme-corp.com	3.7
21	LOW	Strict-Transport-Security Header...	https://acme-corp.com	3.1
22	LOW	Cookie Without HttpOnly Flag	https://app.acme-corp.com	3.1
23	LOW	Cookie Without Secure Flag	https://app.acme-corp.com	2.6
24	INFO	robots.txt Exposed	https://acme-corp.com	-
25	INFO	WAF Detected - Cloudflare	https://acme-corp.com	-
26	INFO	Nginx Version Detected	https://api.acme-corp.com	-