RAPID

PLATFORM Y PRODUCTS Y SERVICES Y RESOURCES Y COMPANY Y PARTNERS

 $\mathsf{EN} \mathrel{ee}$

△ SIGN IN

Blog

Vulnerability Management

MDR

Detection & Response

Cloud Security

App Security

Metasploit

All Topics



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 vulnerability, this blog post will evolve, too.

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 ", a chaining of CVE-2022-41080 and CVE-2022-41082 to bypass URL rewrite mitigations that Microsoft provided for 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.

Rapid7 recommends that organizations who have yet to install the Exchange update (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

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.



Topics

Metasploit (654)

Vulnerability
Management (359)

Research (236)

Detection and Response

(205)

Vulnerability Disclosure

(148)

Emergent Threat

Response (141)

Cloud Security (136)

Security Operations (20)

Popular Tags

Q Search Tags

Metasploit

Metasploit Weekly

Wrapup

Vulnerability

Management

Research

Logentries

Detection and Response

Accept Cookies

Decline Cookies

X

You can always review and change your cookie preferences through our cookie settings page. For more

ini ormation, piease read our **Privacy Statement Cookies Settings Detection &** Vulnerability Cloud START TRIAL Blog **MDR** Metasploit Management Response Security Security **Topics READ** Exploited in Zero- Microsoft Exchange Server 2019 **MORE** Day Attacks **IOCs** Multiple Vulnerabilities in In addition to the detection rules included in InsightIDR Common Unix **READ Printing System** for Rapid7 customers, other IOCs include: **MORE** (CUPS) PowerShell spawned by IIS ('w3wp.exe') creating High-Risk outbound network connections Vulnerabilities in Common 45.76.141[.]84 READ Enterprise 45.76.143[.]143 **MORE** Technologies Example command being spawned by IIS (w3wp.exe): CVE-2024-40766: Critical Improper **Access Control**

Vulnerability

SonicWall Devices

Affecting

READ

MORE

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

Rapid7 has evidence of exploitation in the wild as far back

as December 1, 2022

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

You can always review and change your cookie preferences through our cookie settings page. For more

infamaatian mlaaaa waad asii Dubaaasi Otataasaa

Blog Vulnerability MDR Detection & Cloud App Metasploit All Topics Q START TRIAL

InsightVM and Nexpose

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

InsightIDR

InsightIDR customers can look 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
- Attacker Technique Renamed Plink
- 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

AUTHOR

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

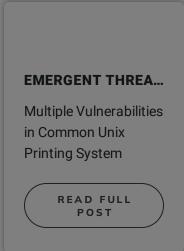
You can always review and change your cookie preferences through our cookie settings page. For more

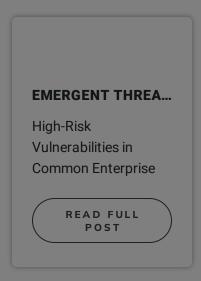
information where word our Buttonic Chatemant

Blog Vulnerability MDR Detection & Cloud App Metasploit All Topics Command Topics Command Topics Command Topics Command Comman

Related Posts









VIEW ALL POSTS

The Commerce of the Composition of the Compo

The Command
Platform

Exposure Command

Managed Threat

Complete

Company **Product Support** Diversity, Equity, and **Resource Library** Inclusion **Our Customers** Leadership **Events & Webcasts News & Press Releases Training & Certification Public Policy** Cybersecurity **Open Source Fundamentals Investors ☑ Vulnerability & Exploit Database**

Contact

Blog

Support Login

Careers Ø

in X f

BACK TO TOP

© Rapid7 Legal Terms Privacy Policy

Do Not Sell or Share My Personal Information

Export Notice Trust

Rapid7 uses cookies and similar technologies as strictly necessary to make our site work. We and our partners would also like to set additional cookies to analyze your use of our site, to personalize and enhance your visit to our site and to show you more relevant content and advertising. These will be set only if you accept.

 $You \ can \ always \ review \ and \ change \ your \ cookie \ preferences \ through \ our \ cookie \ settings \ page. \ For \ more$

infamaatian mlaaaa waad asii Dubaaasi Otataasaa