


# 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.*

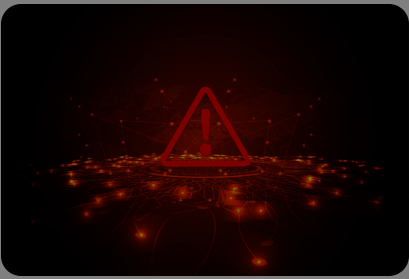
Beginning December 20, 2022, Rapid7 has responded to an increase in the number of Microsoft Exchange server compromises. Further investigation aligned these attacks to what CrowdStrike is reporting as “[OWASSRF](#) ”, a chaining of CVE-2022-41080 and CVE-2022-41082 to bypass URL rewrite mitigations that 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



### 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

- 🔍 Search Tags
- Metasploit
- Metasploit Weekly Wrapup
- Vulnerability Management
- Research
- Logentries
- Detection and Response

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, please read our [Privacy Statement](#).

Accept Cookies

Decline Cookies







information, please read our [Privacy Statement](#)

## Related Posts

EMERGENT THREA...

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

READ FULL POST

EMERGENT THREA...

Multiple Vulnerabilities in Common Unix Printing System

READ FULL POST

EMERGENT THREA...

High-Risk Vulnerabilities in Common Enterprise

READ FULL POST

EMERGENT THREA...

CVE-2024-40766: Critical Improper Access Control

READ FULL POST

VIEW ALL POSTS

Search all the things

BACK TO TOP

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free)

SALES SUPPORT

+1-866-772-7437 (Toll Free)

Need to report an Escalation or a Breach?

⚡ GET HELP

SOLUTIONS

The Command Platform

Exposure Command

Managed Threat Complete

SUPPORT & RESOURCES

Product Support

Resource Library

Our Customers

Events & Webcasts

Training & Certification

Cybersecurity Fundamentals

Vulnerability & Exploit Database

ABOUT US

Company

Diversity, Equity, and Inclusion

Leadership

News & Press Releases

Public Policy

Open Source

Investors

CONNECT WITH US

Contact

Blog

Support Login

Careers

in

X

f

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, please read our [Privacy Statement](#)