Zero-Day Microsoft Exchange Server: Critical Vulnerabilities - OWASSRF and ProxyNotShell

https://campus.barracuda.com/doc/98211382/

This article provides information on recently discovered zero-day vulnerabilities in the Microsoft Exchange Server versions 2013, 2016, and 2019.

The following table provides key information about the vulnerabilities.

Vulnerability	Common Name	Pattern	Mitigation Technique	Barracuda Advisory	Notes
CVE-2022-41040	#proxynotshell	SSRF	Manual Configuration	30 September 2022	First Release
CVE-2022-41082	#proxynotshell	RCE	Manual Configuration	30 September 2022	First Release
CVE-2022-41080	#OWASSRF	RCE	Manual Configuration	22 December 2022	First Release

Description

CVE-2022-41080 & CVE-2022-41082 (#OWASSRF)

Information about these vulnerabilities was discovered by CrowdStrike and first published on 20 December 2022, This exploit affects Microsoft Exchange Server 2013, 2016, and 2019. The attack involves an SSRF equivalent to the Autodiscover technique and the exploit used in the subsequent step of previously identified **#ProxyNotShell**. The exploit provides attackers with access to the PowerShell remoting service through Outlook Web Access instead of previously employed Autodiscover.

Barracuda WAF is not affected by this vulnerability.

#CVE	Criticality & CVSS Score	Exploit Type	Software Firmware Versions	Barracuda WAF Affected
CVE-2022-41080	Zero-Day Critical	RCE	Microsoft Exchange Server 2013, 2016, and 2019	NO
CVE-2022-41082	Zero-Day Critical	RCE	Microsoft Exchange Server 2013, 2016, and 2019	NO

CVE-2022-41040 & CVE-2022-41082 (#ProxyNotShell)

Information about these vulnerabilities was first published on September 29, 2022, and affect Microsoft Exchange Server 2013, 2016, and 2019. An attacker would need to gain access to the vulnerable system as an authenticated user to exploit these vulnerabilities. At first, the SSRF attack is executed to gain access to the PowerShell. Later, the attacker can also execute the RCE attack as described in CVE-2022-41082.

Barracuda WAF is not affected by this vulnerability.

#CVE	Criticality & CVSS Score	Exploit Type	Software Firmware Versions	Barracuda WAF Affected
CVE-2022-41040	Zero-Day Critical	SSRF	Microsoft Exchange Server 2013, 2016, and 2019	NO
CVE-2022-41082	Zero-Day Critical	RCE	Microsoft Exchange Server 2013, 2016, and 2019	NO
CVE-2022-41080	Zero-Day Critical	RCE	Microsoft Exchange Server 2013, 2016, and 2019	NO

Exploit (OWASSRF)

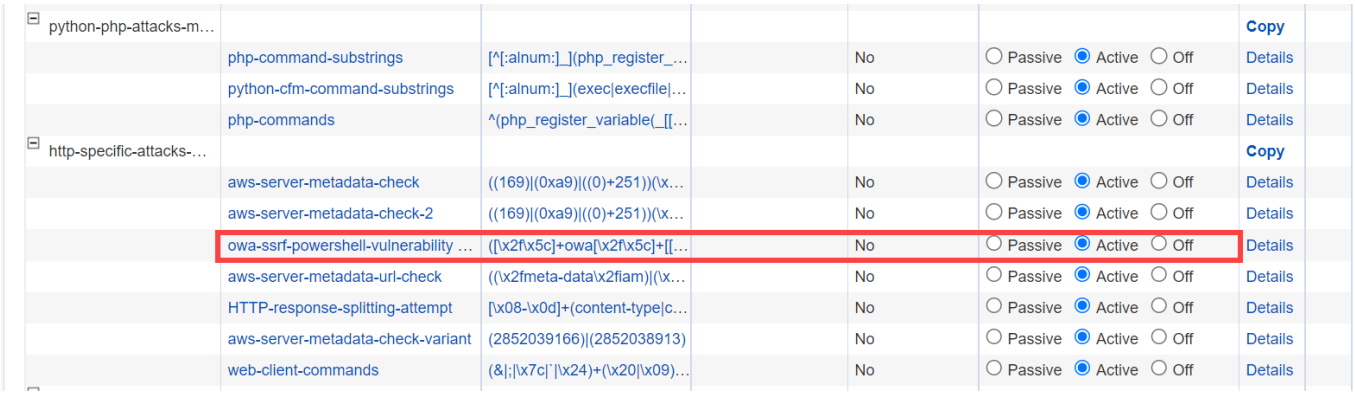
OWASSRF (CVE-2022-41080 & CVE-2022-41082) – Updated on 21 December 2022

CrowdStrike discovered a new exploit method called OWASSRF consisting of 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 through Outlook Web Access (OWA).

Action Required

- Set **Automatic Updates** to **ON** for WAF devices on the **ADVANCED > Energize Updates** page to receive the latest Attack Definition version 1.225.
- Set the **Operating Mode** for the new attack pattern "*owa-ssrf-powershell-vulnerability*" to **Active** in the **ADVANCED > View Internal Patterns > Attack Types > http-specific-attacks-medium** group.

Ensure that the **HTTP Specific Injection** blocked attack type is enabled on the **SECURITY POLICIES > URL Protection** page.



python-php-attacks-m…						Copy
	php-command-substrings	[^[:alnum:]_](php_register_…		No	Passive Active Off	Details
	python-cfm-command-substrings	[^[:alnum:]_](exec|execfile|…		No	Passive Active Off	Details
	php-commands	^(php_register_variable(_[[…		No	Passive Active Off	Details
http-specific-attacks-…						Copy
	aws-server-metadata-check	((169)|(0xa9)|((0)+251))(\x…		No	Passive Active Off	Details
	aws-server-metadata-check-2	((169)|(0xa9)|((0)+251))(\x…		No	Passive Active Off	Details
	owa-ssrf-powershell-vulnerability …	([\x2f\x5c]+owa[\x2f\x5c]+[[…		No	Passive Active Off	Details
	aws-server-metadata-url-check	((\x2fmeta-data\x2fiam)|(\x…		No	Passive Active Off	Details
	HTTP-response-splitting-attempt	[\x08-\x0d]+(content-type|c…		No	Passive Active Off	Details
	aws-server-metadata-check-variant	(2852039166)|(2852038913)		No	Passive Active Off	Details
	web-client-commands	(&|;|\x7c|`|\x24)+(\x20|\x09)…		No	Passive Active Off	Details

Exploit (ProxyNotShell)

CVE-2022-41040 is a Server-Side Request Forgery (SSRF) vulnerability and *CVE-2022-41082* allows Remote Code Execution (RCE) when the Exchange PowerShell is accessible to the attacker.

Barracuda WAF Manual Mitigation Configuration

1. Go to **WEBSITES > Allow/Deny/Redirect**.
2. In the **URL: Allow/Deny/Redirect Rules**, click the **Select** drop-down list next to the service and select **Add**.
3. In the **Create ACL** page:
    1. Enter a name and the URL match.
    2. In **Extended Match**:
        1. Click the edit icon and set the **Element Type** as **URI**, the **Operation** as **regex contains**, and the **Value** as ***.*autodiscover.*.*powershell***
        2. Click **Insert**.
        3. Again, in the **Value**, replace the regex with ***.*powershell.*.*autodiscover***
        4. Change the **Concatenate** option to **or**.
        5. Click **Insert** and **Apply**.
    3. Set **Action** to **Deny and Log**.
    4. Click **Save**.

This may result in some false positives depending on how the application names other parameters. Accordingly, the administrator can create the pattern initially in the **Passive Mode** and review the Web Firewall Logs generated.

Recommendation

As a best practice, it is recommended that you consider interim mitigations and recommendations

from Microsoft to protect your Microsoft Exchange Server.

Vendor Advisory (#OWASSRF):
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41080

Vendor Advisory (#ProxyNotShell):
https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

Related Articles :

#OWASSRF

- https://www.crowdstrike.com/blog/owassrf-exploit-analysis-and-recommendations/
- https://www.rapid7.com/blog/post/2022/12/21/cve-2022-41080-cve-2022-41082-rapid7-observed-exploitation-of-owassrf-in-exchange-for-rce/
- https://socradar.io/reports-of-proxynotshell-vulnerabilities-being-actively-exploited-cve-2022-41040-and-cve-2022-41082/
- https://www.securityweek.com/ransomware-uses-new-exploit-bypass-proxynotshell-mitigations

#ProxyNotShell

- https://www.csa.gov.sg/singcert/Alerts/al-2022-056
- https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html#:~:text=Temporary%20containment%20measures
- https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-new-exchange-zero-days-are-used-in-attacks/
- https://borncity.com/win/2022/09/30/exchange-server-werden-ber-0-day-exploit-angegriffen-29-sept-2022/
- https://thehackernews.com/2022/09/warning-new-unpatched-microsoft.html

Figures