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

https://campus.barracuda.com/doc/98218625/

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 Load Balancer ADC is not affected by this vulnerability.

#CVE	Criticality & CVSS Score	Exploit Type	Software Firmware Versions	Barracuda Load Balancer ADC 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 Load Balancer ADC is not affected by this vulnerability.

#CVE	Criticality & CVSS Score	Exploit Type	Software Firmware Versions	Barracuda Load Balancer ADC 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

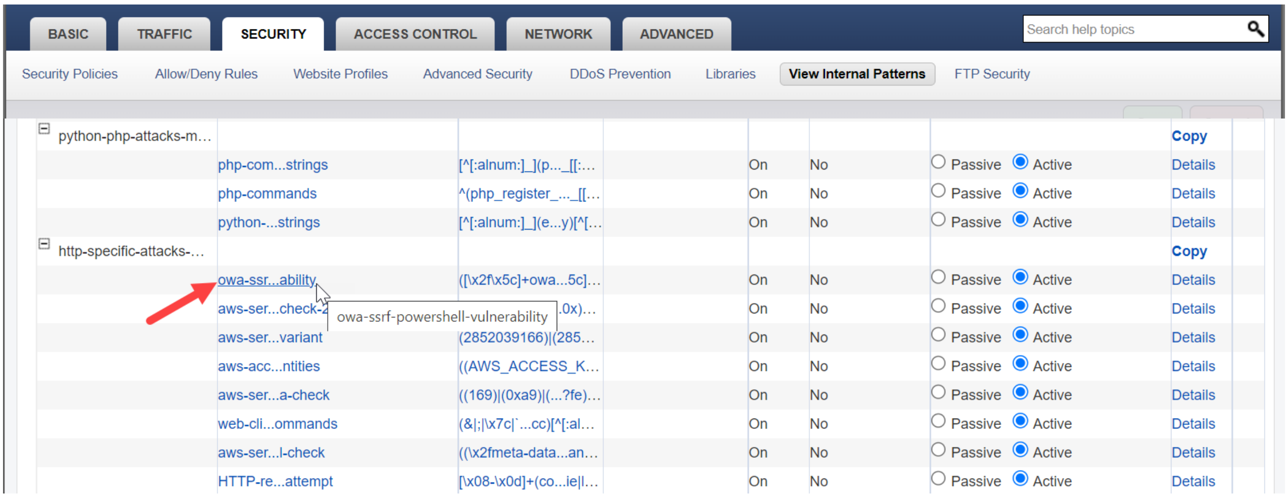
CrowdStrike discovered a new exploit method called OWASSRF consisting of a chaining of CVE-2022-41080 and CVE-2022-41082 to bypass URL rewrite mitigations that Microsoft provided for **ProxyNotShell** allowing for remote code execution (RCE) via privilege escalation through Outlook Web Access (OWA).

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.

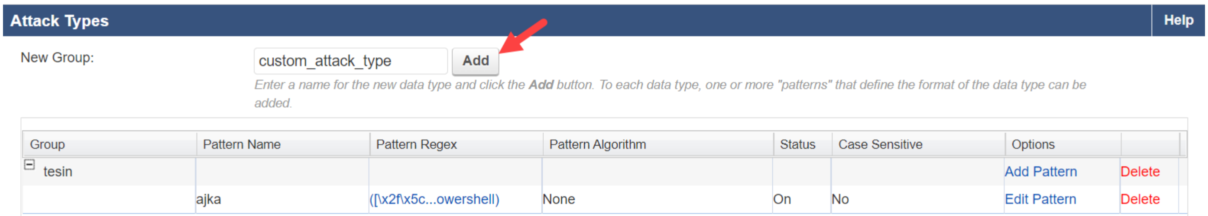
Barracuda Load Balancer ADC Manual Mitigation Configuration

1. Go to the **SECURITY > View Internal Patterns** page, **Attack Types** section.
2. Scroll down to the *http-specific-attacks-medium* group and click **Details** next to the **owa-ssrf-powershell-vulnerability** pattern.



⊟ python-php-attacks-m…						Copy
	php-com...strings	[^[:alnum:]_](p..._[[:…	On	No	○ Passive ● Active	Details
	php-commands	^(php_register_..._[[…	On	No	○ Passive ● Active	Details
	python-...strings	[^[:alnum:]_](e...y)[^[…	On	No	○ Passive ● Active	Details
⊟ http-specific-attacks-…						Copy
	owa-ssr...ability	([\x2f\x5c]+owa...5c]…	On	No	○ Passive ● Active	Details
	aws-ser...check-2	.0x)…	On	No	○ Passive ● Active	Details
	aws-ser...variant	(2852039166)|(285…	On	No	○ Passive ● Active	Details
	aws-acc...ntities	((AWS_ACCESS_K…	On	No	○ Passive ● Active	Details
	aws-ser...a-check	((169)|(0xa9)|(...?fe)…	On	No	○ Passive ● Active	Details
	web-cli...ommands	(&|;|\x7c|`...cc)[^[:al…	On	No	○ Passive ● Active	Details
	aws-ser...l-check	((\x2fmeta-data...an…	On	No	○ Passive ● Active	Details
	HTTP-re...attempt	[\x08-\x0d]+(co...ie|l…	On	No	○ Passive ● Active	Details

3. In the **Attack Types** pop-up window, copy the **Pattern Regex**.
4. Go to the **SECURITY > Libraries** page, **Attack Types** section.
    1. Enter a name in the **New Group** text field and click **Add**.

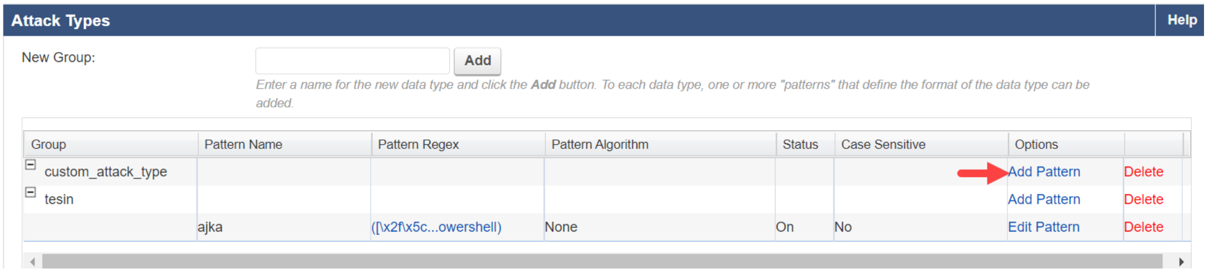


New Group: custom_attack_type

*Enter a name for the new data type and click the **Add** button. To each data type, one or more "patterns" that define the format of the data type can be added.*

Group	Pattern Name	Pattern Regex	Pattern Algorithm	Status	Case Sensitive	Options	
⊟ tesin						Add Pattern	Delete
	ajka	([\x2f\x5c...owershell)	None	On	No	Edit Pattern	Delete

    2. Click **Add Pattern** next to the group you created.



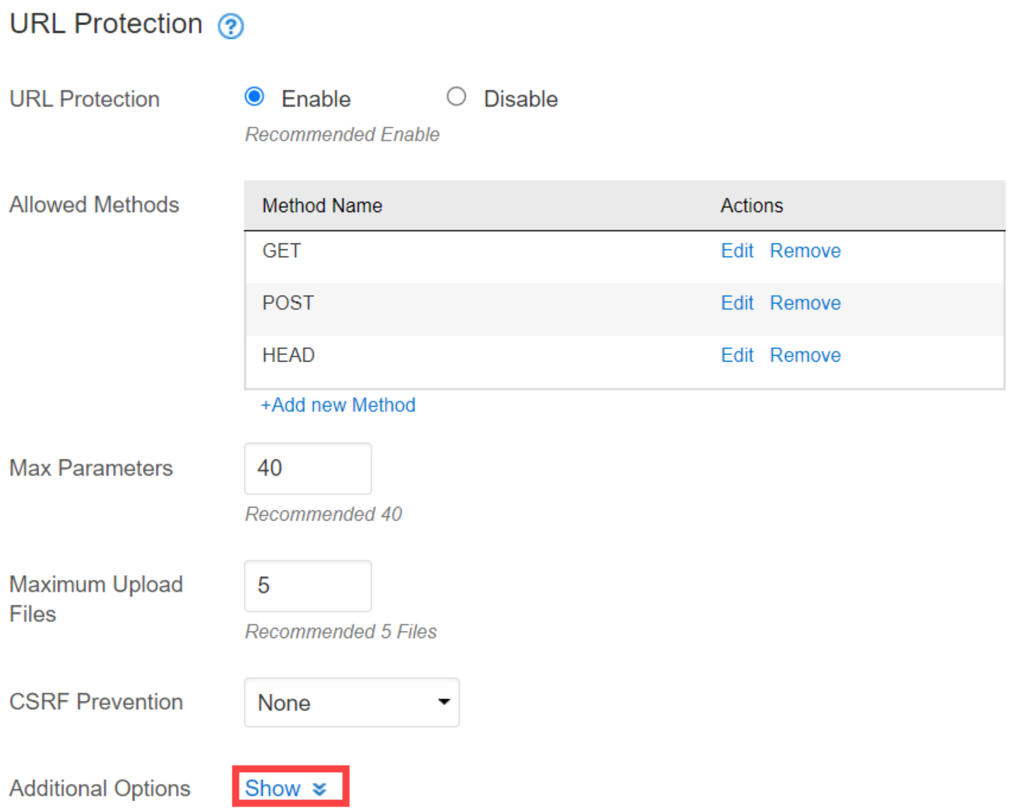
New Group:

*Enter a name for the new data type and click the **Add** button. To each data type, one or more "patterns" that define the format of the data type can be added.*

Group	Pattern Name	Pattern Regex	Pattern Algorithm	Status	Case Sensitive	Options	
⊟ custom_attack_type						Add Pattern	Delete
⊟ tesin						Add Pattern	Delete
	ajka	([\x2f\x5c...owershell)	None	On	No	Edit Pattern	Delete

    3. In the **Attack Types** pop-up window:
        1. Enter a name for the pattern.
        2. Paste the regex that you copied in **step 3** in **Pattern Regex**.
        3. Specify values for other parameters as required and click **Save**.
5. Go to the **SECURITY > Security Policies** page and select the policy the security policy to enable the custom attack type.

6. Scroll down to **URL Protection** and click **Show** to expand **Additional Options**.



URL Protection

URL Protection ● Enable ○ Disable

Recommended Enable

Allowed Methods

Method Name	Actions
GET	Edit Remove
POST	Edit Remove
HEAD	Edit Remove

+Add new Method

Max Parameters: 40

Recommended 40

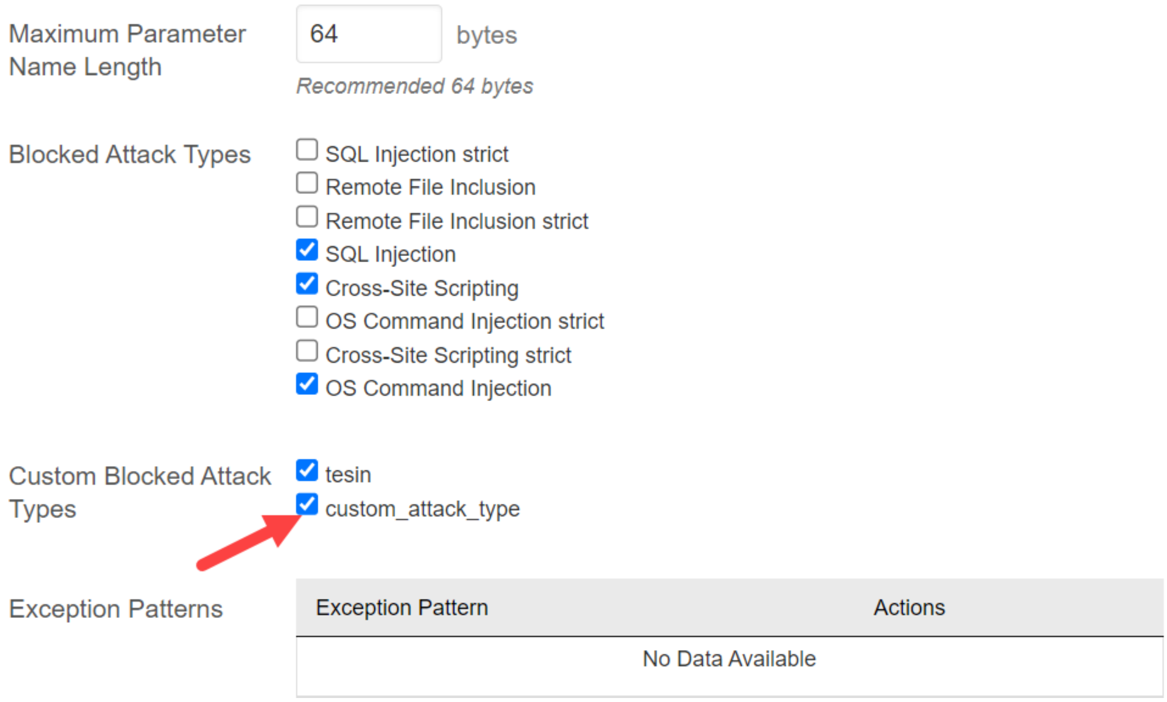
Maximum Upload Files: 5

Recommended 5 Files

CSRF Prevention: None

Additional Options: Show

7. Select the attack type group that you created in **step 4**.



Maximum Parameter Name Length: 64 bytes

Recommended 64 bytes

Blocked Attack Types

□ SQL Injection strict
□ Remote File Inclusion
□ Remote File Inclusion strict
☑ SQL Injection
☑ Cross-Site Scripting
□ OS Command Injection strict
□ Cross-Site Scripting strict
☑ OS Command Injection

Custom Blocked Attack Types

☑ tesin
☑ custom_attack_type

Exception Patterns

Exception Pattern	Actions
No Data Available	

8. Click **Save Changes**.

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