Executive summary

On September 30, 2022, Microsoft released customer guidance reporting two new zero-day flaws that specifically affect versions 2013, 2016, and 2019 of Microsoft's Windows Exchange email servers. The vulnerability has been named CVE-2022-41040 (0-Day SSRF vulnerability in Microsoft Exchange Server) and CVE-2022-41082 (Remote Code Execution vulnerability).

- **CVE-2022–41040 :** Server Side Request Forgery (SSRF) vulnerability. This vulnerability allows an authenticated attacker to remotely trigger the second vulnerability, CVE-2022-41082.

CVSS 3.x Severity and Metrics: 8.8 HIGH

- **CVE-2022–41082 :** This vulnerability allows Remote Code Execution (RCE) when an attacker can access PowerShell.

CVSS 3.x Severity and Metrics: 8.8 HIGH

Introduction

Server-Side Request Forgery (SSRF) is an attack that involves attackers gaining access to an application that supports importing data from URLs. It allows them to abuse the functionality of a server or replace URLs with new ones. When an attacker checks the URLs, they can issue commands to the servers to read data to the tampered/modified URL. An attacker can use this type of attack to trick the server into sending malicious requests to other servers or services accessible by the server, such as internal network services or databases.

Remote Code Execution (RCE) involves an attacker executing malicious code on systems remotely. Once the hacker gets into the system through the RCE vulnerability, they can execute malware and even take full control over the affected system.

These vulnerabilities are called **ProxyNotShell** vulnerabilities. ProxyNotShell is not a single vulnerability, but a collection of vulnerabilities that can be chained to take control of Microsoft Exchange email servers. ProxyNotShell vulnerabilities are considered zero-day vulnerabilities because they affect the latest versions of Exchange Servers.

- **CVE-2022–41040 :**

  CVE-2022-41040 is a 0-day SSRF vulnerability in Microsoft Exchange Servers. The exploit could also allow an attacker to remotely trigger CVE-2022-41082. Flaw received a CVSS score of 8.8 out of 10. (https://nvd.nist.gov/vuln/detail/CVE-2022-41040)

Associated CVE ID	CVE-2022-41040
Description	A 0-Day SSRF Vulnerability in Microsoft Exchange Server
Associated ZDI ID	–
CVSS Score	8.8 High
Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Impact Score	–
Exploitability Score	–
Attack Vector (AV)	Network
Attack Complexity (AC)	Low
Privilege Required (PR)	Low
User Interaction (UI)	None
Scope	Unchanged
Confidentiality (C)	High
Integrity (I)	High
availability (a)	High

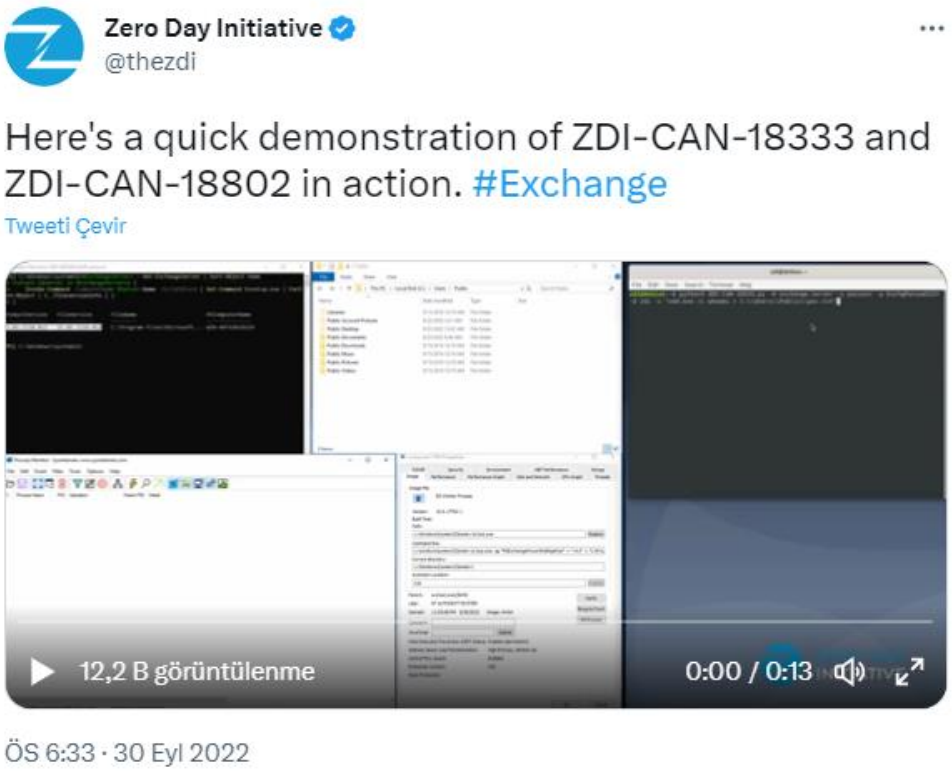
- **CVE-2022–41082**

  CVE-2022-41082 is an RCE vulnerability that can be exploited remotely by an authenticated attacker. Flaw received a CVSS score of 8.8 out of 10. (https://nvd.nist.gov/vuln/detail/cve-2022-41082)

Associated CVE ID	CVE-2022-41082
Description	A RCE Vulnerability in Microsoft Exchange Server
Associated ZDI ID	–
CVSS Score	8.8 High
Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Impact Score	–
Exploitability Score	–
Attack Vector (AV)	Network
Attack Complexity (AC)	Low
Privilege Required (PR)	Low
User Interaction (UI)	None
Scope	Unchanged
Confidentiality (C)	High
Integrity (I)	High
availability (a)	High

- **ZDI** has provided a proof-of-concept video demonstrating the remote attack and execution of a system command with system privileges.

  (https://twitter.com/thezdi/status/1575871397867712512)



Explanation of the vulnerability with its impact

Server-Side Request Forgery (SSRF) is an attack that involves attackers gaining access to an application that supports importing data from URLs. It allows them to abuse the functionality of a server or replace URLs with new ones. When an attacker checks the URLs, they can issue commands to the servers to read data to the tampered/modified URL. An attacker can use this type of attack to trick the server into sending malicious requests to other servers or services accessible by the server, such as internal network services or databases. These types of attacks can be used to gain access to sensitive information or launch other types of attacks, such as denial-of-service (DoS) attacks.

Remote Code Execution (RCE) involves attackers executing malicious code on systems remotely. Once the hacker gets into the system through the RCE vulnerability, they can execute malware and even take full control over the affected system.

Explanation of the exploit

When Microsoft researchers disclosed vulnerability CVE-2022-41040 and CVE-2022-41082 to the Microsoft Security Response Center (MSRC) in September 2022 by the Zero Day Initiative (ZDI) to determine if there is a new exploit vector on the exchange. investigating these attacks.

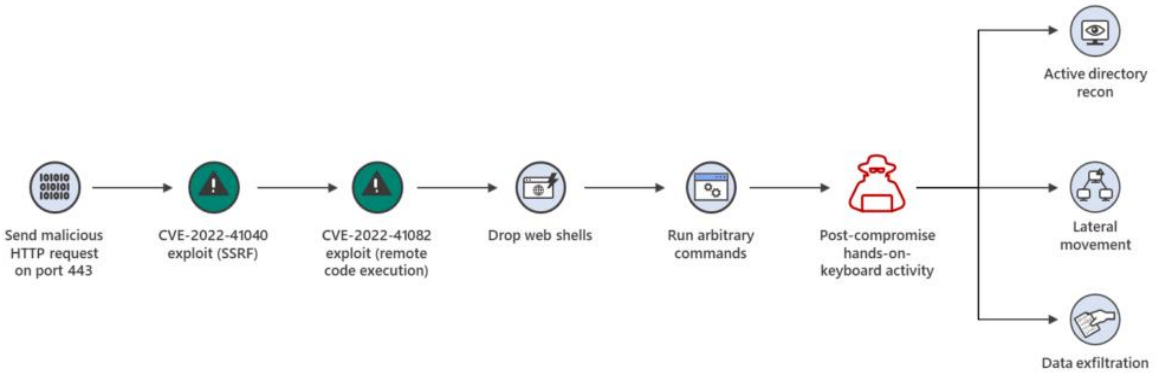


Diagram of attacks using exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082

according to Microsoft

- Usage of CVE-2022-41040 (https://github.com/numanturle/CVE-2022-41040)

  » git clone https://github.com/numanturle/CVE-2022-41040
  cd CVE-2022-41040
  nuclei -u https://target -t owa.yaml

  » `GET/autodiscover/autodiscover.json?@mail.xxx/BACKENDAPI?&Email=autodiscover/autodiscover.json%3f@mail.xxx HTTP/1.1`

```
» Host: mail.xxx
» User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
» Accept: */*
» Connection: close
```

- Usage of CVE-2022-41082 (https://github.com/balki97/OWASSRF-CVE-2022-41082-POC)

  » ## https://sploitus.com/exploit?id=DF35E634-51B1-5A30-AB0B-8518E3754609
  » # CVE-2022-41082-POC
  » PoC for the CVE-2022-41082 NotProxyShell OWASSRF Vulnerability Effecting Microsoft Exchange Servers

  » This is Post-Auth RCE for ProxyNotShell OWASSRF, valid cardentials are needed for command execution.

  » # Affected versions
  » Exchange 2013,16,19 till 08.11.2022 patch
  » This exploit bypasses Microsoft Hotfix from October 2022

  » # Setup
  » ```
  » pip install -r requirements.txt
  » ```

  » # Running
  » ```
  » usage: python poc.py [-H Target] [-u username] [-p "password"] [-c cmd_file]
  » python poc.py -H https://192.168.0.1 -u user2 -p "123QWEasd!@#" -c cmd_file'
  » ```

Current exploitation status (relevant threat groups, attack campaigns)

Threat researcher Dray Agha discovered and leaked online tools for a threat actor. The leaked tool included a proof-of-concept (PoC) for Play's Exchange exploit, allowing CrowdStrike to replicate the malicious activity recorded in Play ransomware attacks.

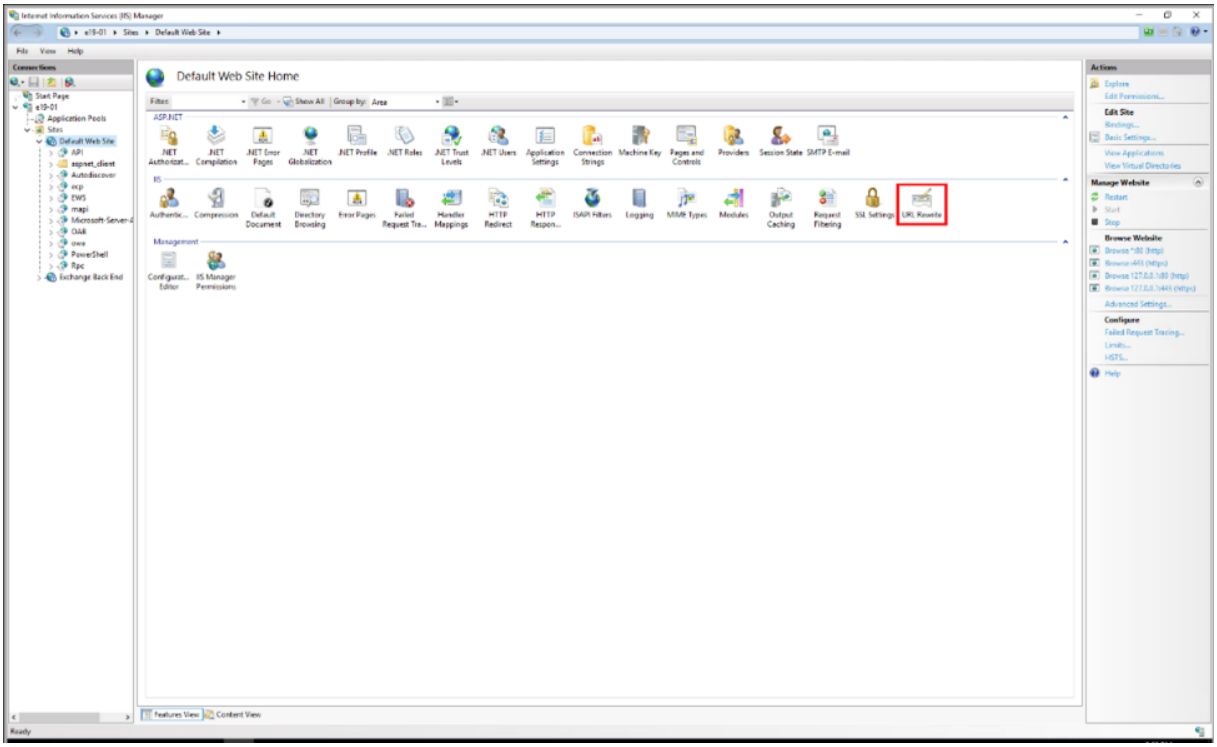
CrowdStrike is believed to be a proof-of-concept exploit used to install remote access programs such as Plink and AnyDesk on infected servers.

Additionally, BleepingComputer discovered that the ConnectWise remote administration program was included in Agha's leaked toolkit and possibly used in attacks.

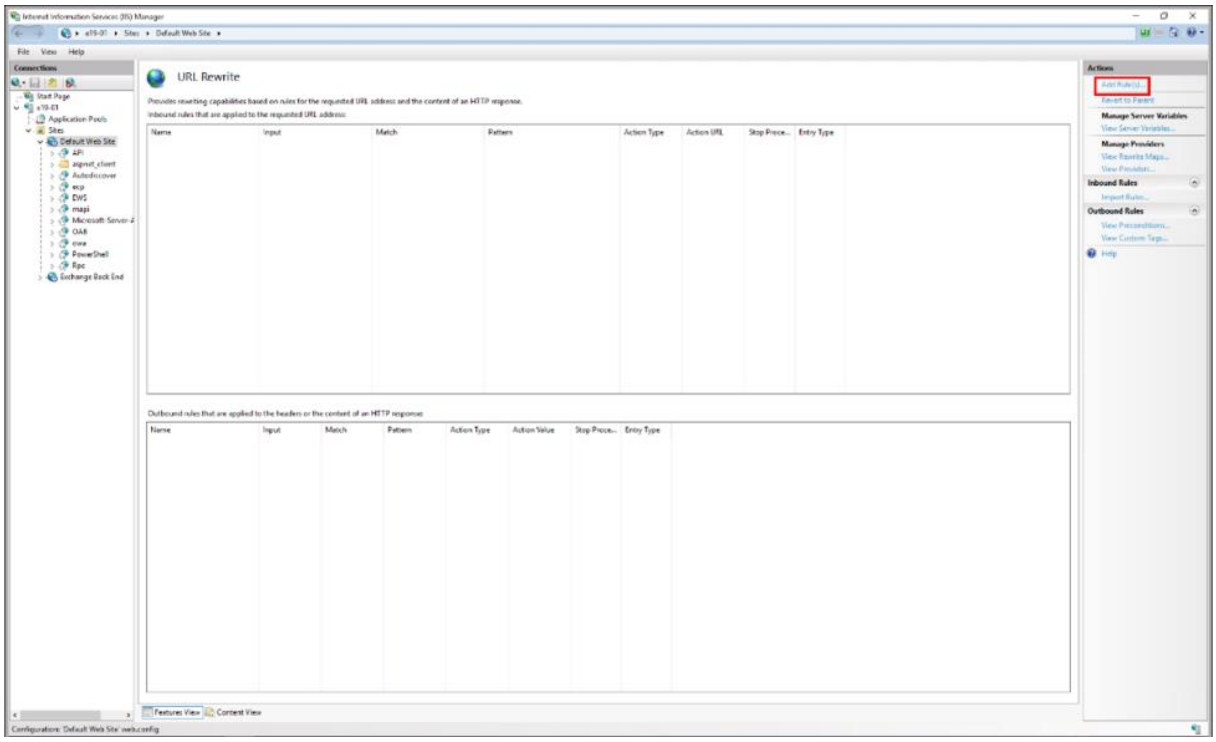
Mitigation suggestions

It has been suggested by Microsoft to add a blocking rule to "IIS Manager -> Default Website -> URL Rewrite -> Actions" to block attacks using vulnerabilities CVE-2022-41040 and CVE-2022-41082. These steps are described below.

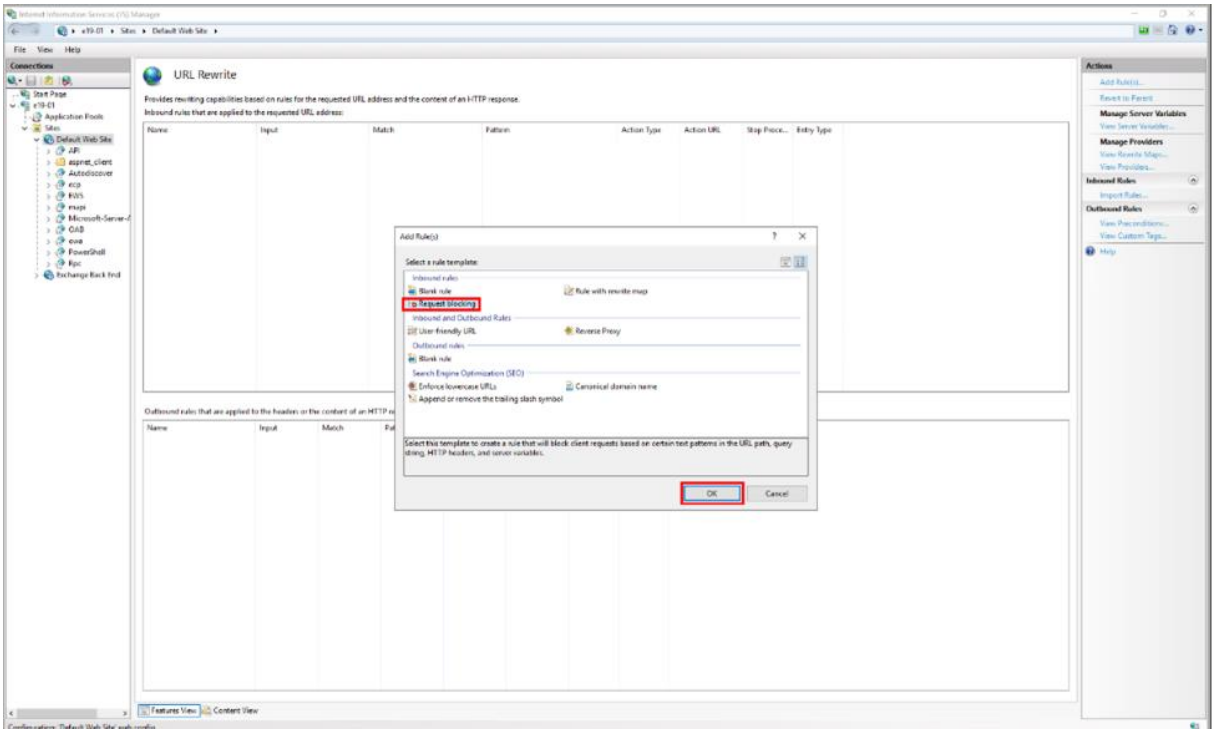
- Open IIS Manager, select Default Website, click URL Rewrite in Feature View.



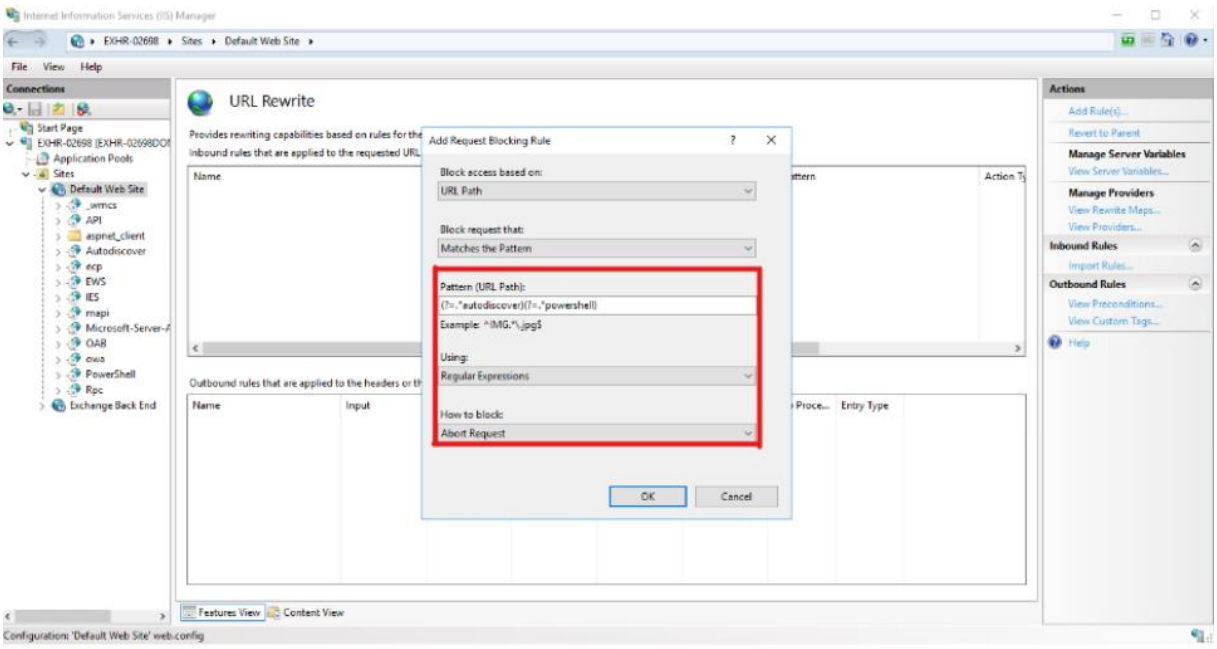
- In the Actions pane on the right, click Add Rule(s)



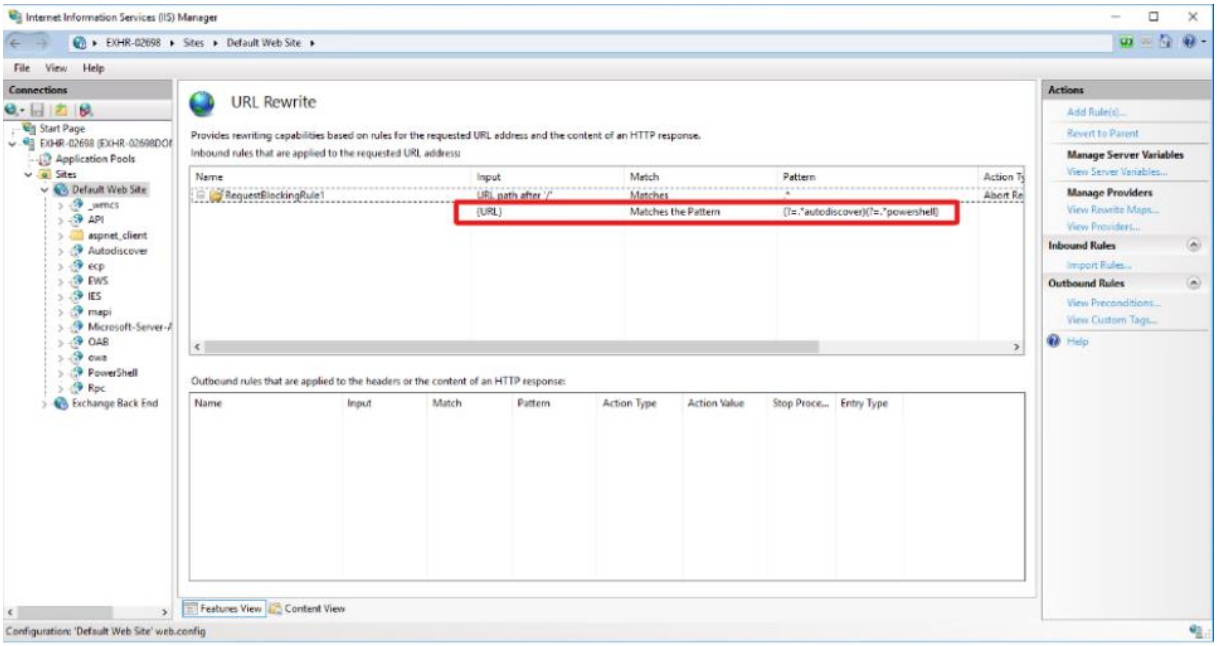
- Select Request Blocking and click OK.



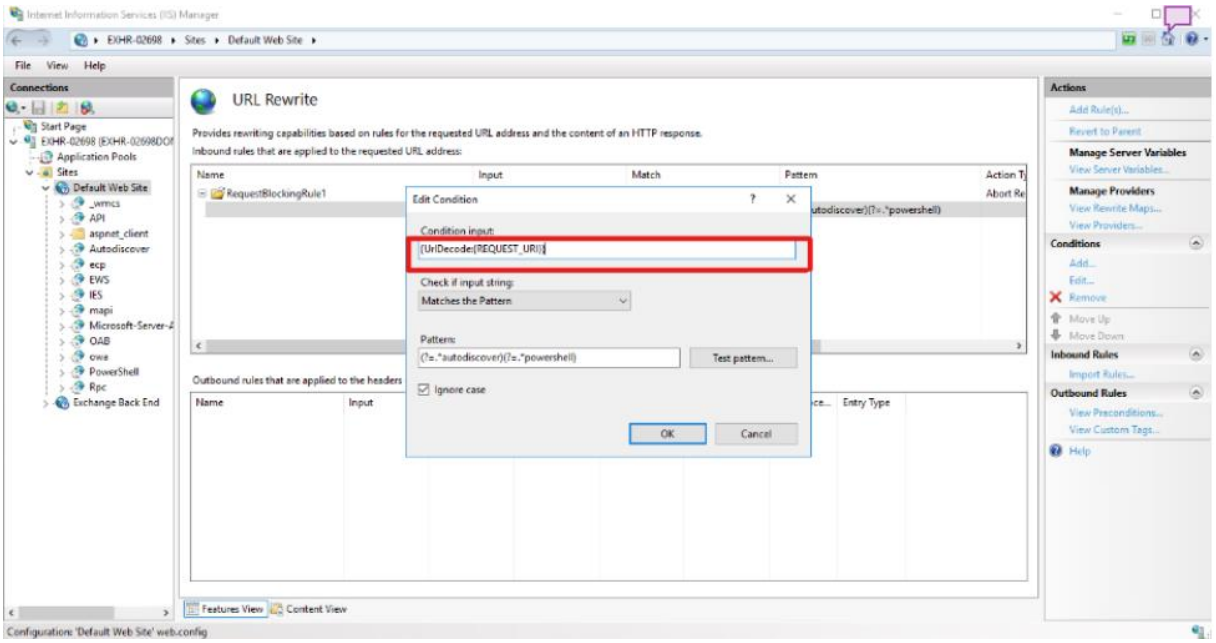
- The string " (?=.*autodiscover)(?=.*powershell) " is added. Use Regular Expression is selected under Under How to block, select Cancel Request and then click OK.



- Expand the rule and select the rule with the pattern: (?=.*autodiscover)(?=.*powershell). Click Edit under Conditions.



- Change the Condition input from {URL} to {UrlDecode:{REQUEST_URI}} and then click OK.



- Remote PowerShell access is disabled for non-administrators.

  (https://learn.microsoft.com/en-us/powershell/exchange/control-remote-powershell-access-to-exchange-servers?view=exchange-ps&viewFallbackFrom=exchange-ps%22%20%5Cl%20%22use-the-exchange-management-shell-to-enable-or-disable-remote-powershell-access-for-a-user)

- On November 8, Microsoft also released security updates for two zero-day vulnerabilities affecting Microsoft Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019. Organizations are encouraged to protect their organizations by immediately applying updates to affected systems.

Conclusion

Vulnerabilities CVE-2022-41040 and CVE-2022-41082 in Microsoft Exchange Server are chained to increase the attack surface. If an attacker uses the first, they can also trigger the second. It allows any attacker to process the malware execution and even have full control over the affected system.

Microsoft has released security updates for vulnerabilities CVE-2022-41040 and CVE-2022-41082 on November 8, 2022. Organizations are encouraged to protect their organizations by immediately applying updates to affected systems.

I hope this article will help you learn how to mitigate an SSRF vulnerability CVE-2022-41040 and RCE CVE-2022-41082 vulnerability in Microsoft Exchange Server.