TLP:WHITE
Szabadon terjeszthető!

Riasztás
Microsoft Exchange szervereket érintő sérülékenységről

(2022. szeptember 30.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet **riasztást** ad ki **Microsoft Exchange** szervereket érintő **magas kockázati besorolású sérülékenységek kapcsán**, mivel azt a támadók aktívan kihasználják. Sikeres kihasználás esetén a megfelelő jogosultsággal rendelkező támadó távoli kódfuttatást vihet végbe az érintett szerveren. A sérülékenységek jelenleg nem rendelkeznek önálló CVE számmal.

Az esetet felfedő kiberbiztonsági kutatók szerint a sérülékenység nem érinti azokat, akik nem helyi eléréssel futtatják a Microsoft Exchange programot, illetve nincs a nyílt interneten használt Outlook Web App.

A z érintettség felfedésére az alábbi módszer áll rendelkezésre:

- IIS naplófájl (%SystemDrive%\inetpub\logs\LogFiles) vizsgálata az alábbi parancson keresztül:
    - *Get-ChildItem -Recurse -Path <Path_IIS_Logs> -Filter "*.log" | Select-String -Pattern 'powershell.*autodiscover\.json.*\@.*200*

A sérülékenység vonatkozásában jelenleg nem áll rendelkezésre javítás, az NBSZ NKI javasolja a kapcsolódó IoC-k tiltását a határvédelmi rendszeren:

Webshell:

File Name: pxh4HG1v.ashx

SHA256: c838e77afe750d713e67ffeb4ec1b82ee9066cbe21f11181fd34429f70831ec1

Path: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\pxh4HG1v.ashx

File Name: RedirSuiteServiceProxy.aspx

Hash (SHA256): 65a002fe655dc1751add167cf00adf284c080ab2e97cd386881518d3a31d27f5

Path: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\RedirSuiteServiceProxy.aspx

File Name: RedirSuiteServiceProxy.aspx

Hash (SHA256): b5038f1912e7253c7747d2f0fa5310ee8319288f818392298fd92009926268ca

Path: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\RedirSuiteServiceProxy.aspx

File Name: Xml.ashx

Hash (SHA256): c838e77afe750d713e67ffeb4ec1b82ee9066cbe21f11181fd34429f70831ec1

Path: Xml.ashx

Filename: errorEE.aspx

SHA256: be07bd9310d7a487ca2f49bcdaafb9513c0c8f99921fdf79a05eaba25b52d257

Path: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\errorEE.aspx

DLL:

File name: Dll.dll

SHA256:

074eb0e75bb2d8f59f1fd571a8c5b76f9c899834893da6f7591b68531f2b5d82

45c8233236a69a081ee390d4faa253177180b2bd45d8ed08369e07429ffbe0a9

9ceca98c2b24ee30d64184d9d2470f6f2509ed914dafb87604123057a14c57c0

29b75f0db3006440651c6342dc3c0672210cfb339141c75e12f6c84d990931c3

c8c907a67955bcdf07dd11d35f2a23498fb5ffe5c6b5d7f36870cf07da47bff2

File name: 180000000.dll (Dump từ tiến trình Svchost.exe)

SHA256: 76a2f2644cb372f540e179ca2baa110b71de3370bb560aca65dcddbd7da3701e

TLP:WHITE
Szabadon terjeszthető!

IP:

125[.]212[.]220[.]48

5[.]180[.]61[.]17

47[.]242[.]39[.]92

61[.]244[.]94[.]85

86[.]48[.]6[.]69

86[.]48[.]12[.]64

94[.]140[.]8[.]48

94[.]140[.]8[.]113

103[.]9[.]76[.]208

103[.]9[.]76[.]211

104[.]244[.]79[.]6

112[.]118[.]48[.]186

122[.]155[.]174[.]188

125[.]212[.]241[.]134

185[.]220[.]101[.]182

194[.]150[.]167[.]88

212[.]119[.]34[.]11

TLP:WHITE
Szabadon terjeszthető!

URL:

hxxp://206[.]188[.]196[.]77:8080/themes.aspx

C2:

137[.]184[.]67[.]33

Hivatkozások:

- https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html
- https://doublepulsar.com/proxynotshell-the-story-of-the-claimed-zero-day-in-microsoft-exchange-5c63d963a9e9
- https://thehackernews.com/2022/09/warning-new-unpatched-microsoft.html
- https://nki.gov.hu/it-biztonsag/hirek/figyelem-ms-exchange-zero-day-sebezhetoseg-aktiv-kihasznalas-alatt/

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu