# Intelligence Advisory

HAFNIUM targeting Microsoft Exchange Servers with 0-day exploits

**3rd March 2021**

**Severity Level:** Guarded
**Classification**: Public

Date: 3rd March, 2021

# DESCRIPTION

Microsoft has released security updates for Exchange Server 2013, 2016, and 2019, where they fixed 4 actively exploited vulnerabilities. 3 of them could allow remote code execution, and one vulnerability (CVE-2021-26855) could allow server-side request forgery.

The vulnerabilities if exploited could allow the threat actors gain access to the on-premises Exchange servers and also, the victim environment.

Microsoft has attributed this threat activity to "HAFINUM", a China state-sponsored hacking group based on observed tactics and procedures.

The vulnerabilities being exploited are CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065.

Affected Microsoft Exchange Server versions:

· Microsoft Exchange Server 2013
· Microsoft Exchange Server 2016
· Microsoft Exchange Server 2019

# INDICATORS OF COMPROMISE

| IP Addresses |
|---|
| 103[.]77[.]192[.]219 |
| 104[.]140[.]114[.]110 |
| 104[.]250[.]191[.]110 |
| 108[.]61[.]246[.]56 |
| 149[.]28[.]14[.]163 |
| 157[.]230[.]221[.]198 |
| 167[.]99[.]168[.]251 |
| 185[.]250[.]151[.]72 |
| 192[.]81[.]208[.]169 |
| 203[.]160[.]69[.]66 |
| 211[.]56[.]98[.]146 |
| 5[.]254[.]43[.]18 |
| 5[.]2[.]69[.]14 |
| 80[.]92[.]205[.]81 |
| 91[.]192[.]103[.]43 |

| Hashes |
|---|
| b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0 |
| 097549cf7d0f76f0d99edf8b2d91c60977fd6a96e4b8c3c94b0b1733dc026d3e |
| 2b6f1ebb2208e93ade4a6424555d6a8341fd6d9f60c25e44afe11008f5c1aad1 |
| 65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5 |
| 511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1 |
| 4edc7770464a14f54d17f36dc9d0fe854f68b346b27b35a6f5839adf1f13f8ea |
| 811157f9c7003ba8d17b45eb3cf09bef2cecd2701cedb675274949296a6a183d |
| 1631a90eb5395c4e19c7dbcbf611bbe6444ff312eb7937e286e4637cb9e72944 |

| Filenames |
|---|
| web[.]aspx |
| help[.]aspx |
| document[.]aspx |
| errorEE[.]aspx |
| errorEEE[.]aspx |
| errorEW[.]aspx |
| errorFF[.]aspx |
| healthcheck[.]aspx |
| aspnet_www[.]aspx |
| aspnet_client[.]aspx |
| xx[.]aspx |
| shell[.]aspx |
| aspnet_iisstart[.]aspx |
| one[.]aspx |

| File Paths |
|---|
| C:\inetpub\wwwroot\aspnet_client\ |
| C:\inetpub\wwwroot\aspnet_client\system_web\ |
| %PROGRAMFILES%\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\ |
| C:\Exchange\FrontEnd\HttpProxy\owa\auth\aspnet_iisstart[.]aspx |
| one[.]aspx |

# RECOMMENDED ACTIONS

nsfLABs recommends the following:

- High priority deployment of March security updates to address these critical security vulnerabilities.
- Priority should be given to Internet-facing Exchange servers, which are at increased risk.
- Please factor in extra servicing time for any Exchange servers that are not running a currently supported Update Rollup (UR) or Cumulative Update (CU). Any Exchange servers that are not up to date will need to have a supported UR or CU installed before you can install any new security updates.
- Keep applications and operating systems running at the current released patch level.
- Analyse Firewall and Internet proxy logs for the presence of mentioned IOCs.
- Update the Anti-malware solutions at endpoint and perimeter level solutions to include the given IOCs.
- Deploy Endpoint Detection & Response (EDR) tools to detect latest malwares and suspicious activities on endpoints & servers

# REFERENCES

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

***nsfLABs (a NaijaSecForce/NaijaSecCon initiative) is Nigeria's first private computer emergency response service working with citizens, public entities & private organizations to contain cyber threats and to build a more secure and resilient infrastructure for the Nation.***

***Email: notification@nsflabs.ng***