Hive Pro

THREAT ADVISORY

Magic Hound Exploiting Old Microsoft Exchange ProxyShell Vulnerabilities	TA2022074
Threat Level RED	**Publish Date –** Mar 24, 2022

APT35 aka Magic Hound, an Iranian-backed threat group, has begun using Microsoft Exchange ProxyShell vulnerabilities as an initial attack vector and to execute code through multiple web shells. The group has primarily targeted organizations in the energy, government, and technology sectors based in the United States, the United Kingdom, Saudi Arabia, and the United Arab Emirates, among other countries.

The threat actor exploits the Microsoft Exchange ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) to gain initial access to create web shells and disable antivirus services on the victim's system. To gain persistence in the environment, the threat actor employs both account creation and scheduled tasks. For future re-entry, the account is added to the "remote desktop users" and "local administrator's users" groups. The threat actors use PowerShell to issue multiple commands to disable Windows Defender. Then they create a process memory dump from LSASS.exe that is zipped before exfiltration via web shell. The threat actor uses native Windows programs like "net" and "ipconfig" to enumerate the compromised server. A file masquerading as dllhost.exe is used to access the certain domains for command and control. Therefore, data can be exfiltrated by the threat actor which could potentially resulting in information theft and espionage.

The Microsoft Exchange ProxyShell vulnerabilities have been fixed in the latest updates from Microsoft. Organizations can patch these vulnerabilities using the patch links given below.

The MITRE TTPs commonly used by APT35 are:
TA0001: Initial Access
TA0002: Execution
TA0003: Persistence
TA0004: Privilege Escalation
TA0005: Defense Evasion
TA0006: Credential Access
TA0007: Discovery
TA0011: Command and Control
T1190: Exploit Public-Facing Application
T1003: OS Credential Dumping
T1098: Account Manipulation
T1078: Valid Accounts
T1105: Ingress Tool Transfer
T1036: Masquerading
T1036.005: Masquerading: Match Legitimate Name or Location
T1543: Create or Modify System Process
T1543.003: Create or Modify System Process: Windows Service
T1505: Server Software Component
T1505.003: Server Software Component: Web Shell
T1082: System Information Discovery
T1016: System Network Configuration Discovery
T1033: System Owner/User Discovery
T1059: Command and Scripting Interpreter
T1059.003: Command and Scripting Interpreter: Windows Command Shell

Hive Pro

THREAT ADVISORY

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
APT 35 (Magic Hound, Cobalt Illusion, Charming Kitten, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, ITG18, Phosphorus, Newscaster)	Iran	Afghanistan, Canada, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Morocco, Pakistan, Saudi Arabia, Spain, Syria, Turkey, UAE, UK, USA, Venezuela, Yemen	Defense, Energy, Financial, Government, Healthcare, IT, Oil and gas, Technology, Telecommunications	Information theft and espionage

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-31207	Exchange 2013 CU23 versions before 15.0.1497.15, Exchange 2016 CU19 versions before 15.1.2176.12, Exchange 2016 CU20 versions before 15.1.2242.5, Exchange 2019 CU8 versions before 15.2.792.13, and Exchange 2019 CU9 versions before 15.2.858.9	cpe:2.3:a:microsoft:*:*:*:*:*:*:*:*	Post-auth Arbitrary-File-Write leads to RCE	CWE-254
CVE-2021-34523			Elevation of Privilege on Exchange PowerShell Backend	CWE-269
CVE-2021-34473			Pre-auth Path Confusion leads to ACL Bypass	CWE-94

Indicators of Compromise (IoCs)

Type	Value
Domain	tcp443.msupdate[.]us, kcp53.msupdate[.]us
IPv4	148.251.71[.]182, 107.173.231[.]114
SHA256	12c6da07da24edba13650cd324b2ad04d0a0526bb4e853dee03c094075ff6d1a, 7b5fbbd90eab5bee6f3c25aa3c2762104e219f96501ad6a4463e25e6001eb00b, 559d4abe3a6f6c93fc9eae24672a49781af140c43d491a757c8e975507b4032e, 668ec78916bab79e707dc99fdecfa10f3c87ee36d4dee6e3502d1f5663a428a0, 1604e69d17c0f26182a3e3ff65694a49450aafd56a7e8b21697a932409dfd81e, c5aae30675cc1fd83fd25330cec245af744b878a8f86626d98b8e7fcd3e970f8, 84f77fc4281ebf94ab4897a48aa5dd7092cc0b7c78235965637eeef0908fb6c7
SHA1	3a6431169073d61748829c31a9da29123dd61da8, 6bae2d45bbd8c4b0a59ba08892692fe86e596154, 0f676bc786db3c44cac4d2d22070fb514b4cb64c, 27102b416ef5df186bd8b35190c2a4cc4e2fbf37, 8ece87086e8b5aba0d1cc4ec3804bf74e0b45bee, 4d243969b54b9b80c1d26e0801a6e7e46d2ef03e, da2470c3990ea0862a79149c6036388498da83cd
MD5	cacb64bdf648444e66c82f5ce61caf4b, f0be699c8aafc41b25a8fc0974cc4582, d2f4647a3749d30a35d5a8faff41765e, 5f098b55f94f5a448ca28904a57c0e58, 9a3703f9c532ae2ec3025840fa449d4e, b2fde6dc7bd1e04ce601f57805de415b, 1a5ad24a6880eea807078375d6461f58

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31207
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523

References

https://thedfirreport.com/2022/03/21/apt35-automates-initial-access-using-proxyshell/