Microsoft-365-Defender-Hunting-Queries/Execution/exchange-iis-worker-dropping-webshell.md at master · microsoft/Microsoft-365-Defender-Hunting-Queries

By Louie Mayor

Latest commit

Mar 5, 2021

Exchange Server IIS dropping web shells and other artifacts

This query was originally published in the threat analytics report, "Exchange Server zero-days exploited in the wild".

In early March 2021, Microsoft released patches for four different zero-day vulnerabilities affecting Microsoft Exchange Server. The vulnerabilities were being used in a coordinated attack. For more information on the vulnerabilities, visit the following links:

- CVE-2021-26855
- CVE-2021-26857
- CVE-2021-26858
- CVE-2021-27065

The following query checks for the IIS worker process in Exchange Server dropping files that appear to be the web shells and other threat artifacts observed in known attacks.

More queries related to this threat can be found under the See also section of this page.

Query

```
DeviceFileEvents
| where InitiatingProcessFileName == 'w3wp.exe' | where InitiatingProcessCommandLine contains "MSExc
| where FolderPath has_any ("\\wwwroot\\", "HttpProxy\\owa\\","\\Temporary ASP.NET Files\\")
| where not(FolderPath has_any("\\tmp\\","\\dl3\\"))
| where FolderPath !endswith ".log" | where FolderPath !endswith ".json"
| where FolderPath !endswith ".ini"
| where FolderPath !endswith ".vb"
| where FolderPath !endswith '.tmp'
```

```
| where FolderPath !endswith '.xml'
| where FolderPath !endswith '.js'
```

Category

This query can be used to detect the following attack techniques and tactics (see MITRE ATT&CK framework) or security configuration states.

Technique, tactic, or state	Covered? (v=yes)	Notes
Initial access		
Execution	v	
Persistence	v	
Privilege escalation		
Defense evasion		
Credential Access		
Discovery		
Lateral movement		
Collection		
Command and control		
Exfiltration		
Impact		
Vulnerability		
Exploit		
Misconfiguration		
Malware, component		
Ransomware		

See also

- Reverse shell loaded using Nishang Invoke-PowerShellTcpOneLine technique
- Procdump dumping LSASS credentials
- 7-ZIP used by attackers to prepare data for exfiltration

- Exchange PowerShell snap-in being loaded
- Powercat exploitation tool downloaded
- Exchange vulnerability creating web shells via UMWorkerProcess
- Exchange vulnerability launching subprocesses through UMWorkerProcess
- Base64-encoded Nishang commands for loading reverse shell

Contributor info

Contributor: Microsoft 365 Defender team
