


# Exchange Server IIS dropping web shells and other artifacts

 [github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/Execution/exchange-iis-worker-dropping-webshell.md](https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/Execution/exchange-iis-worker-dropping-webshell.md)

microsoft

## microsoft/Microsoft-365-Defender-Hunting-...



Sample queries for Advanced hunting in Microsoft 365 Defender

 70  
Contributors

 12  
Issues

 1k  
Stars

 417  
Forks



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 "MSEExchange"
| where FolderPath has_any ("\\wwwroot\\",
"httpProxy\\owa\\", "\\Temporary ASP.NET Files\\")
| where not(FolderPath has_any("\\tmp\\", "\\d13\\"))
| 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		

<b>Technique, tactic, or state</b>	<b>Covered? (v=yes)</b>	<b>Notes</b>
------------------------------------	-------------------------	--------------

---

Exploit

---

Misconfiguration

---

Malware, component

---

Ransomware

## **See also**

---

## **Contributor info**

---

**Contributor:** Microsoft 365 Defender team