

What is ProxyShell?

ProxyShell is the name for a chain of three Microsoft Exchange Server vulnerabilities, CVE-2021-34473, CVE-2021-34523 and CVE-2021-31207, that together let an unauthenticated attacker run code on on-premises Exchange. A URL-parsing confusion bypassed authentication, a privilege flaw reached the Exchange PowerShell backend, and a mailbox-export feature wrote a web shell to disk. Microsoft patched it in the April and May 2021 updates; mass exploitation began in August 2021. ProxyNotShell (CVE-2022-41040 and CVE-2022-41082) followed in 2022.

HOW IT WORKS

01 How the attack works

Shown for defensive context, the chain looked like this in logs:

- Requests to ``/autodiscover/autodiscover.json`` containing `@` and a back-end path such as `/mapi/` or `/powershell/` in the query string, which is the path-confusion step.
- PowerShell cmdlets such as `New-MailboxExportRequest` run through that access to export a mailbox item containing an encoded payload to a `.aspx` file under the web root.
- A [web shell](/learn/persistence/what-is-a-web-shell) at that `.aspx` path then gave command execution, followed by credential theft and ransomware deployment in many incidents.

ProxyNotShell (September 2022) repeated the pattern with CVE-2022-41040 (a server-side request forgery in the same autodiscover front end) and CVE-2022-41082 (remote code execution through PowerShell). It needed any valid mailbox credential, which made it "not quite" pre-auth, hence the name.

HOW TO DEFEND

- Install the current Exchange cumulative and security updates. ProxyShell was fixed in the April and May 2021 updates and ProxyNotShell in November 2022. Out-of-support Exchange versions receive no fixes.
- Reduce exposure. Do not publish Exchange PowerShell or administrative endpoints to the internet, and put on-premises Exchange behind authentication at the edge where possible.
- Hunt for unexpected `.aspx` files in Exchange web directories, mailbox export requests nobody approved and `autodiscover.json` requests with `@` and back-end paths in IIS logs.
- Consider migration. Many organizations moved mail to a managed service after these chains, removing the internet-facing on-premises server entirely.

SOURCES

- [1] Microsoft: CVE-2021-34473 security update guide
- [2] Microsoft: CVE-2022-41082 security update guide
- [3] CISA Known Exploited Vulnerabilities Catalog
- [4] MITRE ATT&CK: Exploit Public-Facing Application (T1190)

Find the path to a shell before an attacker does.

`securelayer7.net/learn/web-exploitation/what-is-proxyshell`

[Open online](#)