

ProxyNotShell

CVE-2022-41040 & CVE-2022-41082

Microsoft Exchange



e-mail

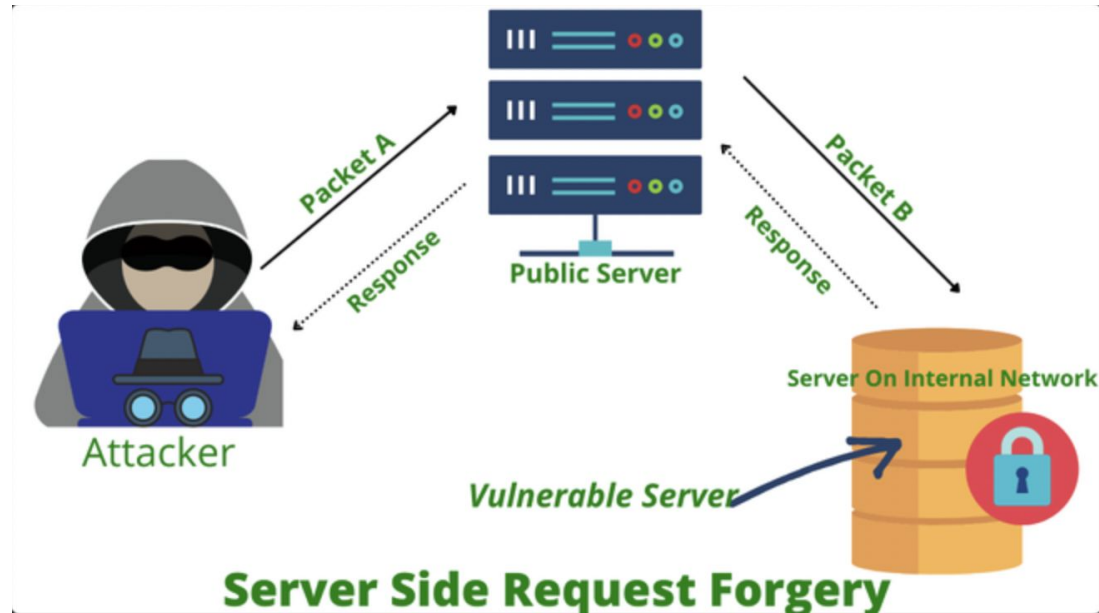
The screenshot shows the Microsoft Exchange email interface. On the left, there's a sidebar with a 'New' button, a search bar, and a 'Folders' list including 'Inbox' (16), 'Sent Items', 'Deleted Items' (54), 'Drafts' (18), 'Apollo', 'Clutter' (19), and 'More'. Below the folders is a 'Groups' section with 'Marketing' (4), 'TechDays', and 'Marketing'. The main area shows the 'INBOX' with a 'Conversations by Date' dropdown. It lists several emails, including one from Garret Vargas about 'Charge code for expenses?' dated 3/30/2015, and another from Tony Krijnen about 'What's Trending' dated 3/9/2015. At the bottom, there's a 'Bing Maps' section showing a map of Chicago with a location marked at 2301 South Lake Shore Drive.

Calendar

The screenshot shows the Microsoft Exchange calendar interface in a weekly view. The top bar includes tabs for 'Personal', 'Birthdays', and 'Bellows College Football'. The calendar grid shows events for the week of October 16 to 19. Key events include 'Erik Nason's Birthda' on Tuesday, 'Show and Tell' at Northwind Elementary School on Wednesday, 'Finance Budget Planning meeting' on Thursday, and 'Marketing Proposal Review' on Friday. A detailed view of a flight event is shown on the right, titled 'Flight to Portland', with details for Contoso Air Lines Flight 415, including the confirmation code J62Y4L and the route from SEA to PDX. The event is scheduled for 9:00 am on October 19 in Seattle, with a return flight at 11:00 am to Portland. A 'View email' link is also visible.

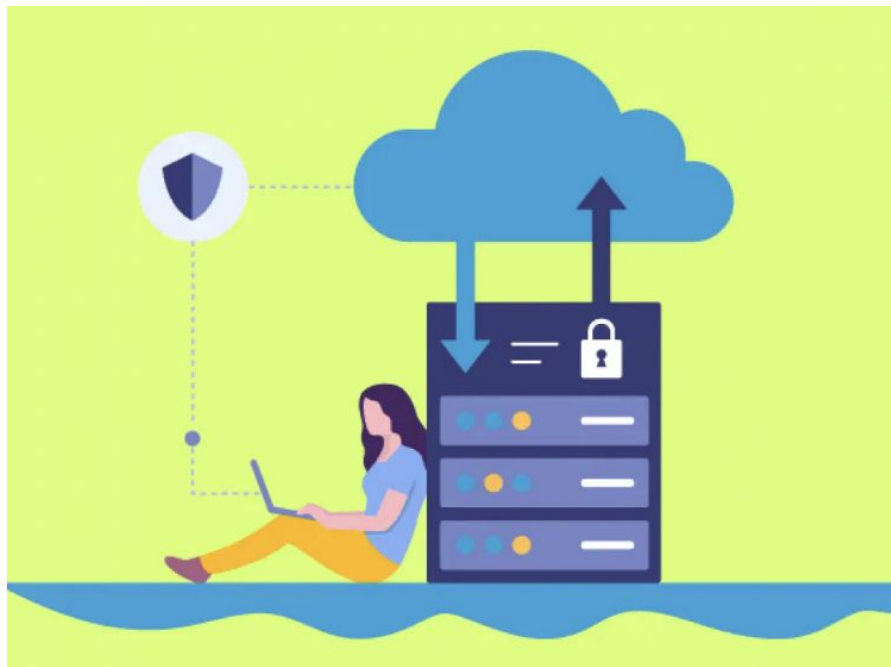
- <https://www.microsoft.com/en-us/microsoft-365/exchange/email>

CVE-2022-41040 - SSRF (Server Side Request Forgery)



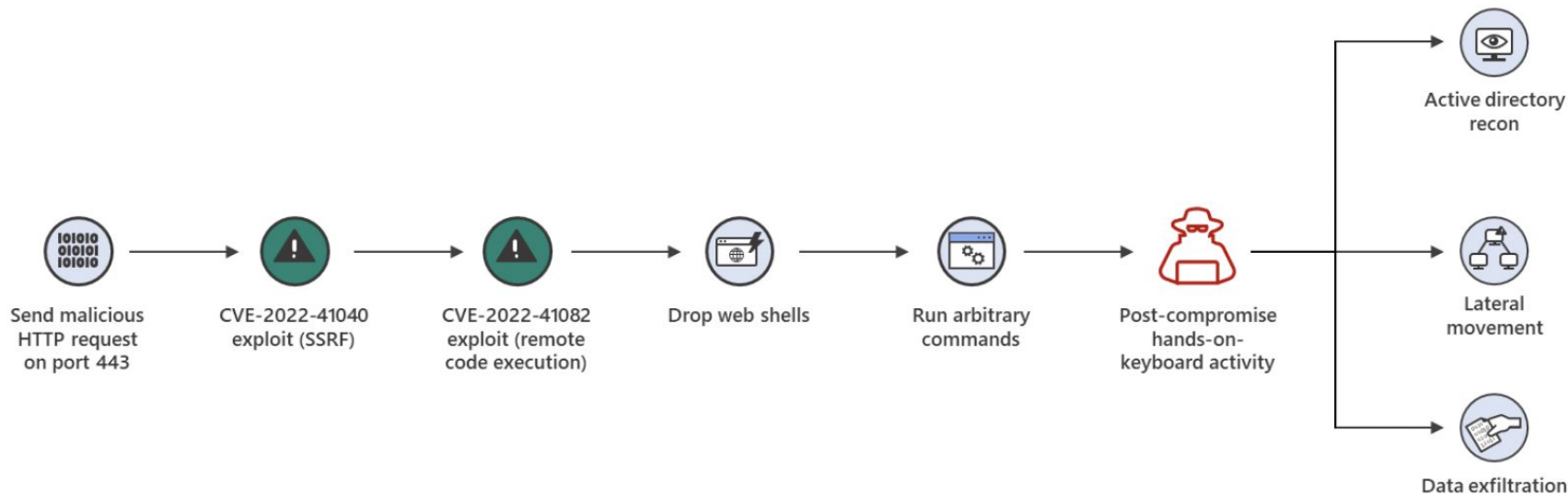
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41040>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040>

CVE-2022-41082 - RCE (Remote Code Execution)



- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41082>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082>

ProxyNotShell Vulnerability



ProxyNotShell Vulnerability

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- PoC <https://github.com/testanull/ProxyNotShell-PoC> (2016 & 2019)


Patching & Mitigations

- <https://www.microsoft.com/en-us/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/>
- <https://learn.microsoft.com/en-us/exchange/exchange-emergency-mitigation-service?view=exchserver-2019>
- <https://techcommunity.microsoft.com/t5/exchange-team-blog/released-november-2022-exchange-server-security-updates/ba-p/3669045>



Microsoft Threat Intelligence Center (MSTIC)

[Recent articles](#) [Products and solutions](#) [Topics](#) [Series](#) [Related blogs](#) [Subscribe](#)




November 22, 2022 • 1 min read

Join us at InfoSec Jupyterthon 2022

Join our community of analysts and engineers at the third annual InfoSec Jupyterthon 2022, an online event taking place on December 2 and 3, 2022.

[Read more](#) >

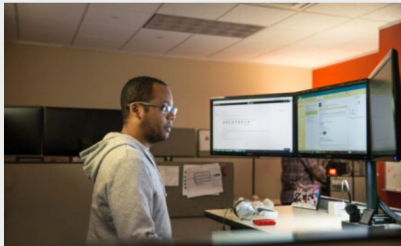


November 22, 2022 • 6 min read

Vulnerable SDK components lead to supply chain risks in IoT and OT environments

As vulnerabilities in network components, architecture files, and developer tools have become an increasingly popular attack vector to leverage access into secure networks and devices, Microsoft identified such a vulnerable component and found evidence of a supply chain risk that might affect millions of organizations and devices.

[Read more](#) >



November 17, 2022 • 7 min read

DEV-0569 finds new ways to deliver Royal ransomware, various payloads

DEV-0569's recent activity shows their reliance on malvertising and phishing in delivering malicious payloads. The group's changes and updates in delivery and payload led to distribution of info stealers and Royal ransomware.

[Read more](#) >

Références

- <https://www.microsoft.com/en-us/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/>
- <https://www.microsoft.com/fr-be/microsoft-365/exchange/email>
- <https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/>
- <https://techcommunity.microsoft.com/t5/exchange-team-blog/released-november-2022-exchange-server-security-updates/ba-p/3669045>

Références

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41082>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41040>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040>
- <https://www.microsoft.com/en-us/security/blog/microsoft-security-intelligence/>
- <https://github.com/testanull/ProxyNotShell-PoC>
- <https://learn.microsoft.com/en-us/exchange/exchange-emergency-mitigation-service?view=exchserver-2019>