#ZERODAY

PROXY NOT SHELL

Informado de forma privada a Microsoft hace tres semanas, **CVE-2022-41040** es una falsificación de solicitud del lado del servidor (SSRF) que permite la escalada de privilegios y funciona con **CVE-2022-41082** para activar la ejecución remota de código en implementaciones de servidor de Exchange en las instalaciones. Ambos problemas de seguridad tienen una puntuación de **GRAVEDAD ALTA** porque explotarlos requiere autenticación.

1

¡Aún no hay un parche! Mientras, sigue las recomendaciones de mitigación. Se basan en el uso de una regla de reescritura de URL para identificar y bloquear los intentos de explotación.

2

La recomendación es deshabilitar el acceso remoto a PowerShell para los que no son administradores.

3

Explotar estas vulnerabilidades solo requiere la autenticación de un usuario estándar.

4

¿Crees que fuiste atacado? GTSC recomienda ejecutar comando de PowerShell para buscar evidencia de intento de explotación.

5

Manténte al día con las medidas de detección y mitigación de tus proveedores de seguridad.

Fuentes:https://www.microsoft.com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/ https://unit42.paloaltonetworks.com/proxynotshell-cve-2022-41040-cve-2022-41082/

Grupo Smartekh

www.smartekh.com