BOLETÍN DE ALERTA

Boletín Nro.: 2022-52
Fecha de publicación: 23/12/2022
Tema: Nuevo método de explotación (OWASSRF) de la vulnerabilidad ProxyNotShell para Microsoft Exchange

Los productos afectados son:

- Exchange Server 2019.
- Exchange Server 2016.
- Exchange Server 2013.

Descripción:

Recientemente se ha reportado un nuevo método de explotación llamado "*OWASSRF*" que aprovecha dos vulnerabilidades (CVE-2022-41080 y CVE-2022-41082) en conjunto conocidas como ProxyNotShell, que afectan a Microsoft Exchange. Las mismas permitirían a un atacante autenticado realizar ejecución remota de código (*RCE*) a través de *Outlook Web Access (OWA*).

El nuevo método de explotación omite las recomendaciones de reescritura de *URL* proporcionado por Microsoft. El mismo está siendo explotado activamente por grupos maliciosos (ej. *Ransomware Play)* y existe una prueba de concepto (PoC) pública de la misma. El método de explotación es similar a los métodos conocidos anteriormente, pero en lugar de apuntar a *AutoDiscover*, se dirige directamente a la interfaz de la aplicación web de Outlook con el fin de obtener acceso remoto a Powershell de Exchange. Las vulnerabilidades afectadas son:

- CVE-2022-41080, de severidad "crítica" y con puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla en el control de elevación de privilegios en Microsoft Exchange Server. Esto permitiría a un atacante obtener escalamiento de privilegios en el sistema afectado, para lograr explotar esta vulnerabilidad el atacante debe contar con credenciales válidas.

- CVE-2022-41082, de severidad "alta" y con puntuación asignada de 8.8. Esta vulnerabilidad se debe a una falla en el componente *PowerShell Handler*. Esto permitiría a un atacante realizar ejecución remota de código (*RCE*) en el sistema afectado, para lo cual necesita previamente estar autorizado.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría realizar escalamiento de privilegios y provocar ejecución de códigos de forma remota.

Solución:

Recomendamos acceder a la actualización de seguridad correspondiente a través de la siguiente guía provista por Microsoft Exchange:

- Actualizaciones de seguridad de Microsoft de Noviembre de 2022.
- Extended Protection - Microsoft - CSS-Exchange

Mitigación:

En caso de no haber aplicado los parches correspondientes, es recomendable seguir los siguientes pasos de mitigación:

- Deshabilitar el acceso remoto a PowerShell para los usuarios que no sean administradores en su organización, a través del siguiente enlace.
- Implementar y configurar herramientas de seguridad tales como *Endpoint Detection and Response* (*EDR*) para detectar servicios web que generen PowerShell o procesos de línea de comandos.
- Supervisar los servidores Exchange en busca de evidencia de explotación visibles en los registros (logs) de IIS y PowerShell mediante el siguiente script.
- Considere implementar de ser posible un firewall de aplicaciones web (*WAF*) para monitorear el tráfico HTTP de las aplicaciones web.

Información adicional:

- https://www.crowdstrike.com/blog/owassrf-exploit-analysis-and-recommendations/
- https://nvd.nist.gov/vuln/detail/CVE-2022-41080
- https://nvd.nist.gov/vuln/detail/CVE-2022-41082
- https://cyware.com/news/beyond-proxynotshell-new-owassrf-exploit-targets-ms-exchange-0d4dae20
- https://www.bleepingcomputer.com/news/security/ransomware-gang-uses-new-microsoft-exchange-exploit-to-breach-servers/
- https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-november-8-2022-kb5019758-2b3b039b-68b9-4f35-9064-6b286f495b1d