Microsoft reveló el viernes que un solo grupo de actividad en agosto de 2022 logró el acceso inicial y violó los servidores de Exchange al encadenar las dos vulnerabilidades de día cero recientemente reveladas en un conjunto limitado de ataques dirigidos a menos de 10 organizaciones en todo el mundo.

> *«Estos ataques instalaron el shell web de Chopper para facilitar el acceso directo al teclado, que los atacantes usaron para realizar el reconocimiento de Active Directory y la exfiltración de datos»,* dijo el Microsoft Threat Intelligence Center (MSTIC) en un informe el viernes.

Se espera que el uso de armas de las vulnerabilidades aumente en los siguientes días, advirtió Microsoft, puesto que los hackers cooptan las vulnerabilidades en sus kits de herramientas, incluida la implementación de ransomware, debido al *«acceso altamente privilegiado que los sistemas de Exchange confieren a un atacante».*

El gigante tecnológico atribuyó los ataques en curso con confianza media a una organización patrocinada por el estado, y agregó que ya estaba investigando estos ataques cuando Zero Day Initiative reveló las vulnerabilidades al Microsoft Security Response Center (MSRC) el 8 y 9 de septiembre de 2022.

Las dos vulnerabilidades se denominaron colectivamente ProxyNotShell, debido al hecho de que *«es la misma ruta y el mismo par SSRF/RCE»* que ProxyShell pero con autenticación, lo que sugiere un parche incompleto.

Las vulnerabilidades, que se unen para lograr la ejecución remota de código, son:

- CVE-2022-41040: Vulnerabilidad de falsificación de solicitud del lado del servidor de Microsoft Exchange Server.
- CVE-2022-41082: Vulnerabilidad de ejecución remota de código de Microsoft Exchange Server.

> *«Aunque estas vulnerabilidades requieren autenticación, la autenticación necesaria para la explotación puede ser la de un usuario estándar. Las credenciales de usuario estándar se pueden adquirir a través de muchos ataques diferentes, como el rociado de contraseñas o la compra por medio de la economía ciberdelincuente»,* dijo Microsoft.

Las vulnerabilidades fueron descubiertas por primera vez por la empresa de seguridad cibernética vietnamita GTSC, como parte de sus esfuerzos de respuesta a incidentes para un cliente en agosto de 2022. Se sospecha que un atacante chino está detrás de las intrusiones.

El desarrollo se produce cuando la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) agregó las dos vulnerabilidades de día cero de Microsoft Exchange Server a su Catálogo de Vulnerabilidades Explotadas Conocidas (KEV), lo que requiere que las agencias federales apliquen los parches antes del 21 de octubre de 2022.

Microsoft dijo que está trabajando en una *«línea de tiempo acelerada»* para lanzar una solución para las deficiencias. También publicó un script para los siguientes pasos de mitigación de reescritura de URL, que según dijo, es *«exitoso para romper las cadenas de ataque actuales»:*

- Administrador de IIS abierto
- Seleccionar sitio web predeterminado
- En la Vista de características, haga clic en Reescritura de URL
- En el panel Acciones en el lado derecho, haga clic en Agregar regla(s)…
- Seleccione Solicitar bloqueo y haga clic en Aceptar
- Agregue la cadena «*.autodiscover.json.*\@.*Powershell.*» (excluyendo las comillas)
- Seleccione Expresión regular en Uso
- Seleccione Cancelar solicitud en Cómo bloquear y luego haga clic en Aceptar
- Expanda la regla y seleccione la regla con el patrón *.autodiscover.json.*\@.*Powershell.* y haga clic en Editar en Condiciones.
- Cambie la entrada de condición de {URL} a {REQUEST_URI}

Como medidas de prevención adicionales, la compañía insta a las empresas a aplicar la autenticación multifactor (MFA), deshabilitar la autenticación heredada y educar a los usuarios sobre cómo lo aceptar solicitudes inesperadas de autenticación de dos factores (2FA).

> *«Microsoft Exchange es un objetivo jugoso para que los actores de amenazas exploten por dos razones principales»,* dijo Travis Smith, vicepresidente de investigación de amenazas de malware en Qualys.

> *«Primero, Exchange [...] al estar conectado directamente a Internet crea una superficie de ataque a la que se puede acceder desde cualquier parte del mundo, lo que aumenta drásticamente el riesgo de ser atacado. En segundo lugar, Exchange es una función de misión crítica: las organizaciones no pueden simplemente desconectarse o apagar el correo electrónico sin afectar gravemente su negocio de forma negativa».*