ProxyToken, vulnerabilidad de Microsoft Exchange Server que permite a los hackers reconfigurar buzones de correo

Autor: I. Stepanenko

Fecha: Wednesday 29th of September 2021 02:55:32 AM

Se han dado a conocer detalles sobre una vulnerabilidad de seguridad ahora parcheada que afecta a Microsoft Exchange Server y que un atacante no autenticado podría utilizar como arma para modificar las configuraciones del servidor, lo que lleva a la divulgación de información de identificación personal (PII).

La vulnerabilidad, rastreada como CVE-2021-33766 con puntuación CVSS de 7.3 y nombrada como ProxyToken, fue descubierta por Le Xuan Tuyen, investigador del Centro de Seguridad de la Información del Grupo de Correos y Telecomunicaciones de Vietnam (VNPT-ISC), e informó a través del programa Zero-Day Initiative (ZDI) en marzo de 2021.

> «Con esta vulnerabilidad, un atacante no autenticado puede realizar acciones de configuración en buzones de correo pertenecientes a usuarios arbitrarios. Como ilustración del impacto, esto puede usarse para copiar todos los correos electrónicos

> dirigidos a un objetivo y una cuenta y reenviarlos a una cuenta controlada por el atacante», dijo la ZDI.

Microsoft abordó el problema como parte de sus actualizaciones de Patch Tuesday para julio de 2021.

La deficiencia de seguridad reside en una función llamada Autenticación Delegada, que se refiere a un mecanismo por el que un sitio web de front-end, el cliente de acceso web de Outlook (OWA), pasa las solicitudes de autenticación directamente al back-end cuando detecta la presencia de una cookie Security Token.

Sin embargo, debido a que Exchange tiene que estar configurado específicamente para usar la función y hacer que el back-end realice las verificaciones, conduce a un escenario en el que el módulo que maneja esta delegación (*«DelegatedAuthModule»*) no se carga con la configuración predeterminada, culminando en un desvío ya que el back-end no puede autenticar las solicitudes entrantes basadas en la cookie Security Token.

> «El resultado neto es que las solicitudes pueden navegar, sin estar sujetas a autenticación en la parte delantera o trasera», explicó Simon Zuckerbraun de ZDI.

La divulgación se suma a una lista cada vez mayor de vulnerabilidades de Exchange Server que han salido a la luz a lo largo de este año, incluyendo ProxyLogon, ProxyOracle y ProxyShell, que han sido explotadas activamente por los hackers para tomar el control de servidores no parcheados, implementar shells web maliciosos y ransomware de cifrado de archivos como LockFile.

Esto preocupa ya que se han registrado intentos de explotación en la naturaleza que abusan de ProxyToken el 10 de agosto, según el investigador de seguridad de NCC Group, Rich Warren, por lo que es imperativo que los clientes apliquen rápidamente las actualizaciones de seguridad de Microsoft.