INFORME: 11CND22-00084-01
TLP: BLANCO

ALERTA DE SEGURIDAD CIBERNÉTICA
VULNERABILIDAD DÍA CERO EN MICROSOFT EXCHANGE

1. Antecedentes generales

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte la información divulgada recientemente por Microsoft sobre dos vulnerabilidades de día cero que afectan a los servidores Exchange de Microsoft en sus versiones 2013, 2016 y 2019.

Las vulnerabilidades fueron descubiertas por una firma de seguridad de Vietnam (GTSC) e informadas globalmente este jueves 29 de septiembre. Esta mañana Microsoft reconoció las vulnerabilidades, así como el procedimiento de mitigación elaborado por GTSC. Microsoft indicó que el número de entidades cuyos servidores han sido explotados son limitados y puso a disposición de la comunidad, a través de su Centro de Respuestas de Seguridad, una guía para sus clientes que sirve como base a este comunicado.

Las vulnerabilidades de día cero han sido identificadas como:

- CVE-2022-41040
  Falsifica solicitudes del lado del servidor (SSRF)

- CVE-2022-41082
  Permite la ejecución remota de código (RCE) cuando el atacante logra acceder a PowerShell

En el comunicado liberado esta mañana por Microsoft, la empresa indica que está trabajando aceleradamente en el parche, por lo que este comunicado será actualizado una vez que esa información esté disponible.

2. Mitigaciones temporales

En su comunicado, Microsoft señaló que los clientes de Exchange Online no necesitan realizar acciones de mitigación, pero si validó las recomendaciones elaboradas originalmente por la firma de seguridad GTSC para mitigar el impacto en el resto de los clientes de Exchage.

Dichas recomendaciones para Exchange Server ya están disponibles en el siguiente enlace: https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

3. Indicadores de Compromiso

El CSIRT de Gobierno solicita a los administradores de revisar y analizar los siguientes Indicadores de Compromiso, los que fueron entregados por GTSC:

- **Webshell:**
  File Name: pxh4HG1v.ashx
  Hash (SHA256): c838e77afe750d713e67ffeb4ec1b82ee9066cbe21f11181fd34429f70831ec1
  Path:
  C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\pxh4HG1v.ashx

  File Name: RedirSuiteServiceProxy.aspx
  Hash (SHA256): 65a002fe655dc1751add167cf00adf284c080ab2e97cd386881518d3a31d27f5
  Path:
  C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\RedirSuiteServiceProxy.aspx

  File Name: RedirSuiteServiceProxy.aspx
  Hash (SHA256): b5038f1912e7253c7747d2f0fa5310ee8319288f818392298fd92009926268ca
  Path:
  C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\RedirSuiteServiceProxy.aspx

  File Name: Xml.ashx
  Hash (SHA256): c838e77afe750d713e67ffeb4ec1b82ee9066cbe21f11181fd34429f70831ec1
  Path: Xml.ashx

  Filename: errorEE.aspx
  SHA256: be07bd9310d7a487ca2f49bcdaafb9513c0c8f99921fdf79a05eaba25b52d257
  Path:
  C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\errorEE.aspx

- **Bibliotecas DLL:**
  File name: Dll.dll
  SHA256:
  074eb0e75bb2d8f59f1fd571a8c5b76f9c899834893da6f7591b68531f2b5d82
  45c8233236a69a081ee390d4faa253177180b2bd45d8ed08369e07429ffbe0a9
  9ceca98c2b24ee30d64184d9d2470f6f2509ed914dafb87604123057a14c57c0
  29b75f0db3006440651c6342dc3c0672210cfb339141c75e12f6c84d990931c3
  c8c907a67955bcdf07dd11d35f2a23498fb5ffe5c6b5d7f36870cf07da47bff2

  File name: 180000000.dll (Dump từ tiến trình Svchost.exe)
  SHA256: 76a2f2644cb372f540e179ca2baa110b71de3370bb560aca65dcddbd7da3701e

- **Direcciones IP:**
  125[.]212[.]220[.]48

5[.]180[.]61[.]17
47[.]242[.]39[.]92
61[.]244[.]94[.]85
86[.]48[.]6[.]69
86[.]48[.]12[.]64
94[.]140[.]8[.]48
94[.]140[.]8[.]113
103[.]9[.]76[.]208
103[.]9[.]76[.]211
104[.]244[.]79[.]6
112[.]118[.]48[.]186
122[.]155[.]174[.]188
125[.]212[.]241[.]134
185[.]220[.]101[.]182
194[.]150[.]167[.]88
212[.]119[.]34[.]11

- URL:
  hxxp://206[.]188[.]196[.]77:8080/themes.aspx

- C2:
  137[.]184[.]67[.]33

4. Recomendaciones

El CSIRT de Gobierno insta a las entidades a seguir las recomendaciones del fabricante y a estar atentos a la inminente publicación de los parches de seguridad para su mitigación.

Adicionalmente, se solicita a los Órganos de la Administración del Estado, las entidades en convenio de colaboración, a las entidades privadas y público en general, que evalúen la posibilidad de suspender el acceso a sus servicios de correo electrónico de Microsoft Exchange On-premise, desde cualquier geolocalización fuera de Chile. Esto se debería mantener mientras no exista un parche definitivo para estas vulnerabilidades, en calidad de medida extrema y entendiendo el contexto específico de explotación de las vulnerabilidades de los servidores Microsoft Exchange en nuestro país conocido en las recientes semanas.

CSIRT
Gobierno
de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.09.30 16:00:27 -03'00'