CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Alerta ante explotación de varias vulnerabilidades por actores asociados a servicio de inteligencia de Rusia

Santiago, 17 de abril de 2021

TLP: BLANCO

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Detalles de la alerta

Este resumen de ciberataques, vulnerabilidades e incidentes de seguridad cibernética tiene como propósito destacar algunos eventos de días pasados para que puedan ser interpretados y discutidos por las diferentes entidades que tengan acceso a su lectura.

Este informe reúne los antecedentes conocidos hasta el día de su publicación. La información consignada en el presente documento es catalogada como TLP BLANCO.

El 15 de abril de 2021, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) del Departamento de Seguridad Nacional (DHS) de Estados Unidos y el Buró Federal de Investigaciones (FBI) compartieron[1] una alerta conjunta sobre la explotación de varias vulnerabilidades conocidas por parte actores del Servicio de Inteligencia Exterior de Rusia (SVR), entre los que se incluyen aquellos conocidos como APT29, Cozy Bear y The Dukes) con el objetivo de comprometer redes de EE.UU. y sus aliados, incluyendo sistemas de gobierno y seguridad nacional.

Según ambas agencias estadounidenses, las vulnerabilidades que están siendo explotadas son las siguientes:

CVE-2018-13379 Fortinet FortiGate VPN[2][3]
CVE-2019-9670 Synacor Zimbra Collaboration Suite[4]
CVE-2019-11510 Pulse Secure Pulse Connect Secure VPN[5][6]
CVE-2019-19781 Citrix Application Delivery Controller and Gateway[7][8]
CVE-2020-4006 VMware Workspace ONE Access[9]

La recomendación es parchar y mantener actualizados todos los sistemas de la organización, en este caso, según los parches entregados por cada proveedor a sus clientes.

Junto a lo anterior, el mismo 15 de abril la Casa Blanca emitió un comunicado atribuyendo[10]

[1] NSA-CISA-FBI Joint Advisory on Russian SVR Targeting U.S. and Allied Networks: https://us-cert.cisa.gov/ncas/current-activity/2021/04/15/nsa-cisa-fbi-joint-advisory-russian-svr-targeting-us-and-allied.
[2] Alerta del CSIRT de Gobierno: https://www.csirt.gob.cl/noticias/comunicado-sobre-el-acceso-no-autorizado-a-las-herramientas-de-fireeye/.
[3] Informe de la NVD: https://nvd.nist.gov/vuln/detail/CVE-2018-13379.
[4] Informe de la NVD: https://nvd.nist.gov/vuln/detail/CVE-2019-9670.
[5] Alerta del CSIRT de Gobierno: https://www.csirt.gob.cl/noticias/comunicado-sobre-el-acceso-no-autorizado-a-las-herramientas-de-fireeye/
[6] Informe de la NVD: https://nvd.nist.gov/vuln/detail/CVE-2019-11510.
[7] Alerta del CSIRT de Gobierno: https://csirt.gob.cl/vulnerabilidades/9vsa-00108-001/.
[8] Informe de la NVD: https://nvd.nist.gov/vuln/detail/CVE-2019-19781.
[9] Informe de la NVD: https://nvd.nist.gov/vuln/detail/CVE-2020-4006.
[10] FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

formalmente a actores del SVR el compromiso de cadena de suministro que ha afectado a productos de SolarWinds desde el año pasado.

Mitigación

Las acciones a seguir recomendadas por el CSIRT de Gobierno como respuesta a estas acciones por parte de actores del SVR son las siguientes:

- Actualizar todos los sistemas y programas indicados en este documento con los respectivos parches de seguridad entregados por sus proveedores. Es importante siempre mantener todo programa al día, siguiendo las instrucciones de las alertas de seguridad compartidas por los proveedores de sus sistemas y por el CSIRT de Gobierno (https://www.csirt.gob.cl/alertas/).

- Revisar sus sistemas y cuentas en búsqueda de indicadores de compromiso que den cuenta de una intrusión.

- Deshabilitar las capacidades de administración externa (VPN) a sistemas críticos.

- Bloquear protocolos obsoletos o no utilizados en el borde de la red y deshabilitarlos en configuraciones de dispositivos cliente.

- Reducir la exposición de la red local, separando los servicios orientados a internet en una red pequeña y aislada.

- Diseñar y mantener actualizados sus planes de recuperación ante incidentes de seguridad informática.

- Incorporar las recomendaciones de ciberseguridad de los diferentes dispositivos y aplicativos utilizados para la prestación de servicios.

- Actualizar los CMS utilizados a las últimas versiones estables y con los parches de seguridad integrados (Wordpress, Joomla, Cpanel, entre otros).

- Actualizar los diferentes webservers y servidores de aplicaciones utilizados a las últimas versiones estables y con los parches de seguridad integrados (Apache, NginX, Caddy, GlassFish, gunicorn, IceWarp, JbossSecureServer, Jetty, Kestrel, Kong, LiteSpeed, Lotus-Domino, Microsoft IIs, openresty, Tableau, entre otros).

- Se recomienda fuertemente aplicar los parches de seguridad a los servidores de correo electrónico en general, pero en particular a los de Microsoft Exchange Server, que han sido golpeados en los días previos por vulnerabilidades críticas que han permitido que terceras partes infecten o comprometan los servidores vulnerables. Aunque el servidor haya sido parchado se debe, de igual manera, revisar e inspeccionar para descartar que haya sido

infectado o comprometido por terceras partes previo al parchado. Siga las recomendaciones en el sitio dedicado para tal efecto por Microsoft[11].

- Realizar los ajustes de robustecimiento necesarios de la capa de seguridad de los webservers y aplicativos SSL/TLS, verificando que no estén presentes protocolos de cifrado débiles, que no haya certificados con SAN compartidos con otra institución que no sea la primaria, y que las bibliotecas activas estén al día en cuanto a sus parches de seguridad. Use por ejemplo testSSL[12] para verificar si su configuración estánen buenas condiciones de seguridad.

Complementariamente, se recomienda establecer un sistema de respaldos de los aspectos más críticos para ser almacenados de manera offline, con el objetivo de prevenir de mejor manera la contaminación o pérdida de estos ante el caso de una infección grave por ransomware, por ejemplo.

El CSIRT de Gobierno solicita a los Órganos de la Administración del Estado que notifiquen los incidentes que puedan llegar a sufrir, según lo indica el Instructivo Presidencial N°8, y que estén vigilantes ante cualquier anomalía que afecte sus sistemas. En este caso, compartir la información es una forma de ayudarnos entre todos a que el ecosistema digital de gobierno y servicios del estado a los ciudadanos se mantenga seguro y disponible.

Recuerde nuestros canales de notificación:

WEB: https://www.csirt.gob.cl
FONO: +56 2 2486 3850, todo el día, todos los días.
EMAIL: soc@interior.gob.cl

[11] Mitigación a vulnerabilidades de Exchange (Microsoft, marzo2021) https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/.
[12] TestSSL: https://gbhackers.com/testssl-sh-tls-ssl-vulnerabilities/.

Enlaces

NSA-CISA-FBI Joint Advisory on Russian SVR Targeting U.S. and Allied Networks: https://us-cert.cisa.gov/ncas/current-activity/2021/04/15/nsa-cisa-fbi-joint-advisory-russian-svr-targeting-us-and-allied

Comunicado sobre el acceso no autorizado a las herramientas de FireEye: https://www.csirt.gob.cl/noticias/comunicado-sobre-el-acceso-no-autorizado-a-las-herramientas-de-fireeye/.

Informe de la NVD: https://nvd.nist.gov/vuln/detail/CVE-2018-13379.

Informe de la NVD: https://nvd.nist.gov/vuln/detail/CVE-2019-9670.

Informe de la NVD: https://nvd.nist.gov/vuln/detail/CVE-2019-11510.

Informe de la NVD: https://nvd.nist.gov/vuln/detail/CVE-2019-19781.

Informe de la NVD: https://nvd.nist.gov/vuln/detail/CVE-2020-4006.

FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

Mitigación a vulnerabilidades de Exchange (Microsoft, marzo 2021): https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/.

TestSSL: https://gbhackers.com/testssl-sh-tls-ssl-vulnerabilities/.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.04.17 18:25:59 -04'00'