PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 11 de mayo de 2022

N° 127-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Conjunto de aplicaciones Android con el troyano Joker resurge en Google Play Store 4

Microsoft destaca correcciones con esfuerzo colectivo a vulnerabilidades y exploits Zero-day en su última actualización. 6

Múltiples vulnerabilidades en productos de Eaton Corporation 8

Vulnerabilidad en varios productos HMI de AVEVA 9

Índice alfabético 10

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 127	Fecha: 11-05-2022
		Página 4 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Conjunto de aplicaciones Android con el troyano Joker resurge en Google Play Store		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código Malicioso		

Descripción

I. DATOS GENERALES:

Malware : Trojan.Joker

Investigadores: Kaspersky

Se ha observado un nuevo conjunto de aplicaciones troyanizadas que se difunden a través de Google Play Store distribuyendo el notorio malware Joker en dispositivos Android comprometidos.

II. EVIDENCIA:

- Joker, un delincuente reincidente, se refiere a una clase de aplicaciones dañinas que se utilizan para la facturación y el fraude de SMS, al mismo tiempo que realizan una serie de acciones elegidas por un pirata informático malintencionado, como robar mensajes de texto, listas de contactos e información del dispositivo.
- A pesar de los intentos continuos por parte de Google para ampliar sus defensas, las aplicaciones se han iterado continuamente para buscar brechas y pasar desapercibidas a la tienda de aplicaciones.
- En un comunicado de prensa, la empresa afectada se ha manifestado:

"Por lo general, se difunden en Google Play, donde los estafadores descargan aplicaciones legítimas de la tienda, les agregan un código malicioso y las vuelven a cargar en la tienda con un nombre diferente", dijo el investigador de Kaspersky Igor Golovin en un informe publicado la semana pasada.

- Un truco disimulado utilizado por Joker para eludir el proceso de investigación de Google Play es hacer que su carga útil maliciosa esté "inactiva" y solo active sus funciones después de que las aplicaciones se hayan activado en Play Store.

III. TEMA:

- Tres de las aplicaciones infectadas con Joker detectadas por Kaspersky hasta finales de febrero de 2022 se enumeran a continuación. Aunque se han eliminado de Google Play, siguen estando disponibles a través de proveedores de aplicaciones de terceros, estas son:
  1. Mensaje de estilo (com.stylelacat.messagearound),
  2. Aplicación de presión arterial (blood.maodig.raise.bloodrate.monitorapp.plus.tracker.tool.health), y
  3. Escáner PDF de la cámara (com.jiao.hdcam.docscanner)

- Esta no es la primera vez que se descubren troyanos de suscripción en los mercados de aplicaciones. El año pasado, las aplicaciones para la tienda de aplicaciones APKPure y un mod de WhatsApp ampliamente utilizado se encontraron comprometidos con un malware llamado Triada.
- Luego, en septiembre de 2021, Zimperium reveló un plan agresivo para ganar dinero llamado GriftHorse, y lo siguió con otro caso de abuso de servicio premium llamado Dark Herring a principios de enero.
- "Los troyanos de suscripción pueden eludir la detección de bosts en los sitios web de servicios pagos y, a veces, suscriben a los usuarios a los servicios inexistentes de los estafadores", dijo Golovin. "Para evitar suscripciones no deseadas, evite instalar aplicaciones de fuentes no oficiales, que es la fuente más frecuente de malware".

IV. CONCLUSIÓN:

- Incluso cuando descargan aplicaciones de las tiendas de aplicaciones oficiales, se recomienda a los usuarios que lean las reseñas, verifiquen la legitimidad de los desarrolladores, los términos de uso y solo otorguen los permisos que sean esenciales para realizar las funciones previstas.
- "El malware Joker es un claro ejemplo del juego del gato y el ratón que ha ocurrido durante años entre las capas de seguridad y los actores maliciosos detrás de él", dijo Richard Melick, director de informes de amenazas de Zimperium.
- "Con cada actualización, se demuestra una y otra vez que la seguridad básica y la administración de dispositivos móviles no son suficientes. Confiando en la suplantación de identidad y la clonación de aplicaciones, Joker continúa pasando por iteraciones de actualizaciones y avances para poder superar la seguridad básica y OEM., dejando en riesgo a los terminales móviles y a los usuarios.

V. RECOMENDACIÓN:

- Realizar periódicamente respaldos de seguridad.
- Contar con una solución de seguridad para usuario constantemente actualizada tanto en dispositivos de escritorio como en móviles conectados en la red.
- Mantener actualizado el sistema operativo, antivirus y navegadores de internet.

Fuentes de información	▪ hxxps://thehackernews.com/2022/05/another-set-of-joker-trojan-laced.html ▪ hxxps://securelist.com/mobile-subscription-trojans-and-their-tricks/106412/

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 127	Fecha: 11-05-2022
		Página 6 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Microsoft destaca correcciones con esfuerzo colectivo a vulnerabilidades y exploits Zero-day en su última actualización.		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

I. DATOS GENERALES:

CVE-2022-26925: Zero Day, vulnerabilidad de suplantación de identidad
CVE-2022-29972: Falla en un conector de datos ODBC de terceros
CVE-2022-22713: Vulnerabilidad de denegación de servicio de Windows Hyper-V

El martes 10/05/2022, Microsoft lanzó correcciones para 74 vulnerabilidades numeradas CVE, incluida una de día cero bajo ataque activo (CVE-2022-26925) y dos vulnerabilidades conocidas públicamente (CVE-2022-29972 y CVE -2022-22713).

II. EVIDENCIA:

- En primer lugar, tenemos CVE-2022-26925 (Windows LSA Spoofing Vulnerability), una vulnerabilidad de suplantación de identidad "importante" en la autoridad de seguridad local (LSA) de Windows que puede convertirse en una "crítica" si se combina con ataques de retransmisión NTLM.
- El director de investigación de ciberamenazas, Kevin Breen de Immersive Labs, señaló:

*"Esta vulnerabilidad (*CVE-2022-26925*) se explota activamente en la naturaleza, permite que un atacante se autentique como usuarios aprobados como parte de un ataque de retransmisión NTLM, lo que permite que los actores de amenazas obtengan acceso a los hash de los protocolos de autenticación".*

"Si bien todos los servidores se ven afectados, los controladores de dominio deben ser una prioridad para la protección ya que, una vez explotados, brindan acceso de alto nivel a los privilegios, a menudo conocidos como 'las llaves del reino".

- De las 74 vulnerabilidades, siete se califican como Críticos, 66 como Importantes y 1 como de gravedad baja. Dos de las fallas se enumeran como conocidas públicamente en el momento del lanzamiento.
- Entre las vulnerabilidades, abarcan 24 ejecuciones remotas de código (RCE), 21 elevaciones de privilegios, 17 divulgaciones de información y 6 vulnerabilidades de denegación de servicio, entre otras. Las actualizaciones suman 36 fallas parchadas en el navegador Microsoft Edge basado en Chromium el 28 de abril de 2022.

III. TEMA:

- Se ha señalado que la calificación de gravedad de la falla se elevaría a 9.8 si se encadenara con ataques de retransmisión NTLM en los Servicios de certificados de Active Directory (AD CS) como PetitPotam.
- Microsoft, que remedió CVE-2022-29972 el 15 de abril, lo etiquetó como "Explotación más probable" en el Índice de explotabilidad, por lo que es imperativo que los usuarios afectados apliquen las actualizaciones lo antes posible.
- La actualización del martes de parches también se destaca por resolver dos vulnerabilidades de escalada de privilegios (CVE-2022-29104 y CVE-2022-29132) y dos de divulgación de información (CVE-2022-29114 y CVE-

2022-29140) en el componente Print Spooler, que ha representado durante mucho tiempo un objetivo atractivo para los atacantes.

IV. CONCLUSIÓN:

- La complejidad de explotar CVE-2022-26925 se considera alta porque la explotación requiere que un atacante se posicione como un atacante en el medio, agregó Satnam Narang, ingeniero de investigación del personal de Tenable, y se unió a Microsoft para instar a los administradores a corregir esta falla, logrando describir medidas adicionales para mitigar los ataques de retransmisión NTLM contra los servicios de certificados de Active Directory.
- En esencia, cualquier usuario autenticado de dominio puede convertirse en administrador de dominio si los servicios de certificados de Active Directory se ejecutan en el dominio. Este es un despliegue muy común. Teniendo en cuenta la gravedad de este error y la relativa facilidad de explotación, no me sorprendería ver ataques activos utilizando esta técnica más temprano que tarde, señaló Dustin Childs, de la iniciativa Zero Day de Trend Micro.

"Estos tipos de vulnerabilidades atraerán potencialmente a los operadores de ransomware, ya que podrían conducir al tipo de exposición de datos críticos que a menudo forman parte de un intento de rescate. También es importante que los equipos de seguridad tengan en cuenta que el rol de NFS no es una configuración predeterminada para los dispositivos de Windows".

V. RECOMENDACIÓN:

- Visitar el sitio web oficial del desarrollador de las unidades de software para verificar las actualizaciones
- Verificar compatibilidad de controladores de software privativo y nuevas actualizaciones
- Actualizar las plataformas disponibles.

Fuentes de información	▪ hxxps://www.helpnetsecurity.com/2022/05/10/cve-2022-26925/ ▪ hxxps://thehackernews.com/2022/05/microsoft-releases-fix-for-new-zero-day.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 127	Fecha: 11-05-2022
		Página 8 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en productos de Eaton Corporation		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

El investigador, Michael Heinzl, ha reportado múltiples vulnerabilidades de severidad MEDIA de tipo secuencias de comandos entre sitios, secuencias de comandos entre sitios reflejadas y neutralización incorrecta de la fórmula en un archivo CSV que afecta a diversos productos de la compañía de gestión de energía Eaton Corporation. La explotación exitosa de estas vulnerabilidades podría permitir que un atacante remoto ejecute código arbitrario utilizando datos que no son de confianza.

2. Detalles:

- La vulnerabilidad identificada como CVE-2021-23282, se debe a que el producto afectado es vulnerable a una vulnerabilidad de secuencias de comandos entre sitios reflejada debido a una validación insuficiente de la entrada de ciertos recursos por parte del software Eaton Intelligent Power Manager (IPM). Un atacante necesitaría acceso a la subred local y la interacción del administrador para comprometer el sistema.
- La vulnerabilidad identificada como CVE-2021-23283, se debe a que producto afectado es vulnerable a una vulnerabilidad de secuencias de comandos entre sitios debido a la validación insuficiente de la entrada del usuario y la codificación incorrecta de la salida para ciertos recursos dentro del software Eaton Intelligent Power Protector (IPP).
- La vulnerabilidad identificada como CVE-2021-23284, se debe a que el producto afectado ha llegado al final de su vida útil, es vulnerable a una vulnerabilidad de secuencias de comandos entre sitios almacenada debido a la validación insuficiente de la entrada de ciertos recursos por parte del software de infraestructura Eaton Intelligent Power Manager Infrastructure (IPM). El atacante necesitaría acceso a la subred local y la interacción del administrador para comprometer el sistema.
- La vulnerabilidad identificada como CVE-2021-23285, se debe a que el producto afectado ha llegado al final de su vida útil, es vulnerable a una vulnerabilidad de secuencias de comandos entre sitios reflejada debido a la validación insuficiente de la entrada de ciertos recursos por parte del software de infraestructura IPM. El atacante necesitaría acceso a la subred local y la interacción del administrador para comprometer el sistema.
- La vulnerabilidad identificada como CVE-2021-23286, se debe a que el producto afectado ha llegado al final de su vida útil, es vulnerable a una inyección de fórmula CSV. La vulnerabilidad existe debido a una sanitización incorrecta de los archivos CSV importados. El atacante necesitaría acceso a la subred local y la interacción del administrador para comprometer el sistema.

3. Productos afectados:

- Eaton Intelligent Power Manager (IPM) v1: todas las versiones anteriores a versión 1.70;
- Eaton Intelligent Power Manager Infrastructure (Infraestructura IPM): todas las versiones, incluida versión 1.5.0 plus205;
- Eaton Intelligent Power Protector (IPP): Todas las versiones anteriores a la versión 1.69 y 166.

4. Solución:

Eaton recomienda actualizar los productos afectados a la última versión disponible que corrige estas vulnerabilidades:

- Actualizar Eaton IPM a la versión 1.70.
- Eaton Intelligent Power Manager Infrastructure (Infraestructura IPM) ha llegado al final de su vida útil, la notificación se ha publicado en: Notificación de ciclo de vida. La transición a IPM Monitor Edition está en curso.
- Actualizar Eaton Intelligent Power Protector (IPP) a la versión v1.69.

Fuentes de información	▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-130-02 ▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-130-03 ▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-130-04

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 127**	**Fecha: 11-05-2022**
		Página 9 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en varios productos HMI de AVEVA		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

El investigador, Giovanni Delvecchio de Aceaspa, ha reportado una vulnerabilidad de severidad ALTA de tipo exposición del recurso a la esfera equivocada que afecta a varios productos HMI de AVEVA. La explotación exitosa de esta vulnerabilidad podría permitir que un usuario autenticado escape del contexto de la aplicación transmitida al sistema operativo y ejecute comandos arbitrarios del sistema operativo.

2. Detalles:

- La vulnerabilidad de tipo exposición del recurso a la esfera equivocada de debe a que el producto expone un recurso a la esfera de control incorrecta, proporcionando a los actores no deseados un acceso inapropiado al recurso. Los recursos, como archivos y directorios, pueden quedar expuestos sin darse cuenta a través de mecanismos como permisos inseguros o cuando un programa opera accidentalmente en el objeto incorrecto. Por ejemplo, un programa puede tener la intención de que los archivos privados sólo se proporcionen a un usuario específico. Esto define efectivamente una esfera de control que pretende evitar que los atacantes accedan a estos archivos privados. Si los permisos de los archivos no son seguros, las partes que no sean el usuario podrán acceder a esos archivos.

  Una esfera de control separada podría requerir efectivamente que el usuario sólo pueda acceder a los archivos privados, pero no a ningún otro archivo en el sistema. Si el programa no garantiza que el usuario sólo solicite archivos privados, es posible que el usuario pueda acceder a otros archivos del sistema.

- La vulnerabilidad identificada como CVE-2022-1467, se debe a que, el sistema operativo Windows se puede configurar para superponer una "barra de idioma" encima de cualquier aplicación. Cuando esta funcionalidad del sistema operativo está habilitada, la interfaz de usuario de la barra de idioma del sistema operativo se podrá ver en el navegador junto con las aplicaciones InTouch Access Anywhere y Plant SCADA Access Anywhere. Es posible manipular la barra de idioma del sistema operativo Windows para iniciar un símbolo del sistema operativo, lo que resulta en un escape de contexto de la aplicación al sistema operativo.

- Esta vulnerabilidad afecta a múltiples sectores de infraestructura crítica como el de la Energía, Química, Manufactura Crítica, Alimentos y Agricultura, y Sistemas de Agua y Aguas Residuales en todo el mundo.

3. Productos afectados:

AVEVA informa que esta vulnerabilidad afecta a todas las versiones de los siguientes productos HMI:
- AVEVA InTouch Access Anywhere;
- AVEVA Plant SCADA Access Anywhere (anteriormente conocido como AVEVA Citect Anywhere y Schneider Electric Citect Anywhere).

4. Solución:

AVEVA recomienda aplicar las siguientes mitigaciones:
- Deshabilitar la barra de idioma de Windows en la máquina del servidor que aloja las aplicaciones InTouch Access Anywhere y Plant SCADA Access Anywhere a menos que sea necesario;
- Crear cuentas de usuario únicas con privilegios mínimos dedicados únicamente al acceso remoto de las aplicaciones InTouch Access Anywhere y Plant SCADA Access Anywhere;
- Utilizar objetos de política de grupo (GPO) del sistema operativo para restringir aún más lo que pueden hacer esas cuentas de usuario únicas;
- Restringir el acceso según la lista de bloqueo recomendada de Microsoft.

Fuentes de información	▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-130-05 ▪ hxxps://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

Índice alfabético

aplicaciones 4
aplicaciones troyanizadas 4
ciberamenazas 6
código malicioso 4
Google Play 4
Kaspersky 4
malware 4
malware Joker 4
objetos de política de grupo (GPO) 9
privilegios 9
protocolos de autenticación 6
ransomware 7
respaldos de seguridad 5
Servicios de certificados de Active Directory (AD CS) 6
sistema operativo 9
suplantación de identidad 5
troyanos 4
vulnerabilidad 8, 9
Vulnerabilidad 6
Windows Hyper-V 6