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, 15 de noviembre de 2022

310-2022-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

Vulnerabilidad en Android permitía acceder al dispositivo con la pantalla bloqueada. 4
Múltiples fallas de alta gravedad afectan el software de servidor web LiteSpeed 6
Vulnerabilidad crítica de escalada de privilegios locales en el Kernel de Linux. 8
Nuevos hashes maliciosos 9
Múltiples vulnerabilidades en Cisco Identity Services Engine 10
Vulnerabilidad crítica en GT SoftGOT2000 de Mitsubishi Electric Corporation 12
Índice alfabético 13

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 310	Fecha: 15-11-2022
		Página 4 de 13

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidad en Android permitía acceder al dispositivo con la pantalla bloqueada.		
Tipo de ataque	Vulnerabilidad	Abreviatura	Vulnerabilidad
Medios de propagación	Dispositivos Android		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de Intrusión		

Descripción

Google corrigió en la actualización de noviembre de 2022 una vulnerabilidad reportada en junio de 2022 por el investigador David Schütz, quien, realizando unas pruebas en sus dispositivos móviles, un Pixel 6 y un Pixel 5 de Google, descubrió que era posible desbloquear un teléfono y esquivar los mecanismos de bloqueo de pantalla, como son la huella digital o la clave PIN.

La vulnerabilidad fue registrada como CVE-2022-20465 y afecta a los dispositivos que tengan instalada la versión 10, 11, 12 y 13 de Android que no tengan instalados los parches de la actualización de noviembre.

ANTECEDENTES:

- El reconocido experto en ciberseguridad, David Schütz (aka xdavidhu), encuentra una vulnerabilidad que, según el afecta a toda la gama de Google Pixel. Este descubrimiento se realizó en un dispositivo Google Pixel 6 y Google Pixel 5 pero asegura que si se encuentra con cualquier modelo del dispositivo Google Pixel podría desbloquearlo sin problema, esto puede ser replicable en otros dispositivos Android.
- Tras darse cuenta de este error, Schütz, se puso en contacto con Google para informar sobre lo sucedido a buena noticia es que la compañía publicó una actualización con parches para arreglar esta vulnerabilidad, en este caso esta vulnerabilidad encontrada ha sido catalogada como CVE-2022-20465, actualmente este fallo se encuentra arreglado, lo que significa que su teléfono se encuentra protegido si está actualizado.

DETALLES:

- Según explicó el investigador en una publicación, el hallazgo de esta vulnerabilidad se dio de forma casual. Su Google Pixel se quedó sin batería y se apagó. Luego de cargarlo y encenderlo, tuvo que ingresar la clave PIN de su tarjeta SIM. Luego de tres intentos fallidos, la SIM se bloqueó y necesitaba ingresar la clave PUK. Luego de buscar el envoltorio original de la tarjeta SIM donde tenía la clave PUK e ingresar el código, el sistema solicitó ingresar una nueva clave PIN. Luego de configurar una nueva clave PIN y para sorpresa del investigador, el teléfono no solicitó ingresar la clave PIN de desbloqueo, que es lo que debería suceder luego de reiniciar por razones de seguridad. Solo solicitó escanear la huella digital.
- Luego de darse cuenta de que algo no estaba bien, decidió repetir el proceso varias veces. En uno de esos intentos olvidó reiniciar el dispositivo y con el equipo encendido y la pantalla bloqueada, abrió la bandeja para colocar la tarjeta SIM y reemplazó la tarjeta SIM por otra y realizó el mismo proceso: ingreso tres veces una clave PIN incorrecta, luego ingresó la clave PUK, creó una nueva clave PIN y de repente pasó algo inesperado: "**Estaba con la pantalla desbloqueada y con acceso al dispositivo**".
- Tal como explica el investigador, el impacto de este fallo es muy serio. Si bien es necesario acceso físico al dispositivo, el hecho de que un atacante solo necesite una tarjeta SIM y el código PUK para desbloquear un dispositivo expone a las personas a que terceros malintencionados tengan acceso a la información que contiene el smartphone. Pensemos por ejemplo quienes son víctimas del robo de sus teléfonos o quienes son blanco de espionaje.
- Hasta el lanzamiento de la actualización de noviembre el fallo estuvo sin ser parcheado durante al menos seis meses y no hay información acerca de si fue aprovechado por actores malintencionados. Las versiones de Android afectadas por esta vulnerabilidad son Android 10 y versiones posteriores.

RECOMENDACIONES:

- Mantener actualizado su dispositivo Android 10 y versiones posteriores con los últimos parches de seguridad a noviembre 2022.

Fuentes de información	▪ hxxps://blog.segu-info.com.ar/2022/11/encontro-una-vulnerabilidad-en.html ▪ hxxps://www.welivesecurity.com/la-es/2022/11/14/vulnerabilidad-android-evadir-bloqueo-pantalla-acceder-dispositivo/ ▪ hxxps://source.android.com/docs/security/bulletin/2022-11-01#system ▪ hxxps://nvd.nist.gov/vuln/detail/CVE-2022-20465 ▪ Análisis propio de fuentes abiertas.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 310	Fecha: 15-11-2022
		Página 6 de 13

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Múltiples fallas de alta gravedad afectan el software de servidor web LiteSpeed		
Tipo de ataque	Abuso de privilegios o de políticas de seguridad	Abreviatura	AbuPrivPolSeg
Medios de propagación	Red, Internet		
Código de familia	K	Código de subfamilia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

FECHA DEL EVENTO:

El día 15 de noviembre 2022, mediante un informe de la Unit 42 de Palo Alto Networks, se tomó conocimiento de Múltiples Fallas que afectan el software del servidor web OpenLiteSpeed y LiteSpeed Enterprise.

ANTECEDENTES:

LiteSpeed es un servidor web centrado en el rendimiento, existen 1,9 millones de instancias de dicho servidor en línea.

DETALLES:

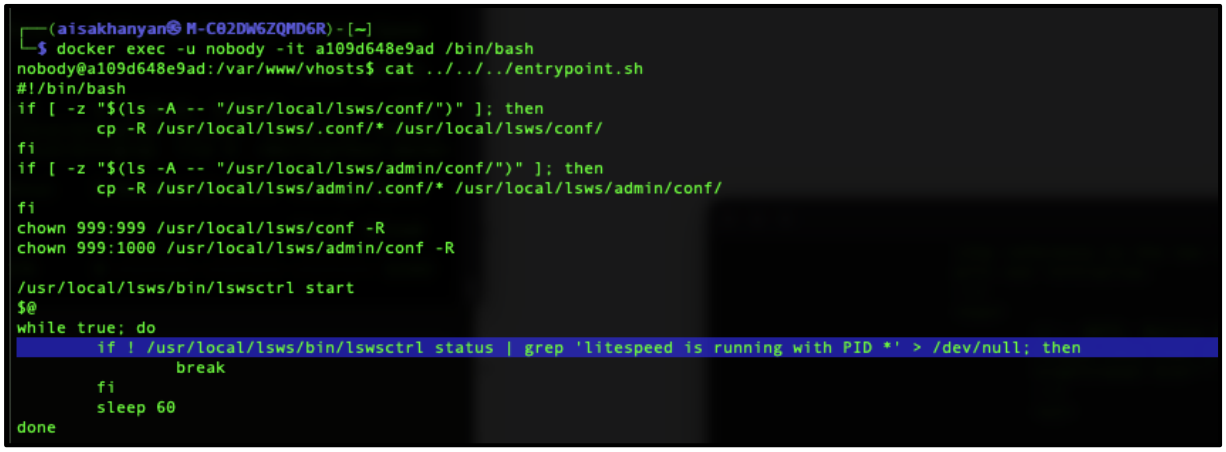
El equipo de investigación de Unit 42 descubrió tres (03) vulnerabilidades diferentes en el servidor web OpenLiteSpeed de código abierto. Estas vulnerabilidades también afectan a la versión empresarial, LiteSpeed Web Server. Al explotar las vulnerabilidades, los adversarios podrían comprometer el servidor web y obtener una ejecución remota de código con todos los privilegios.

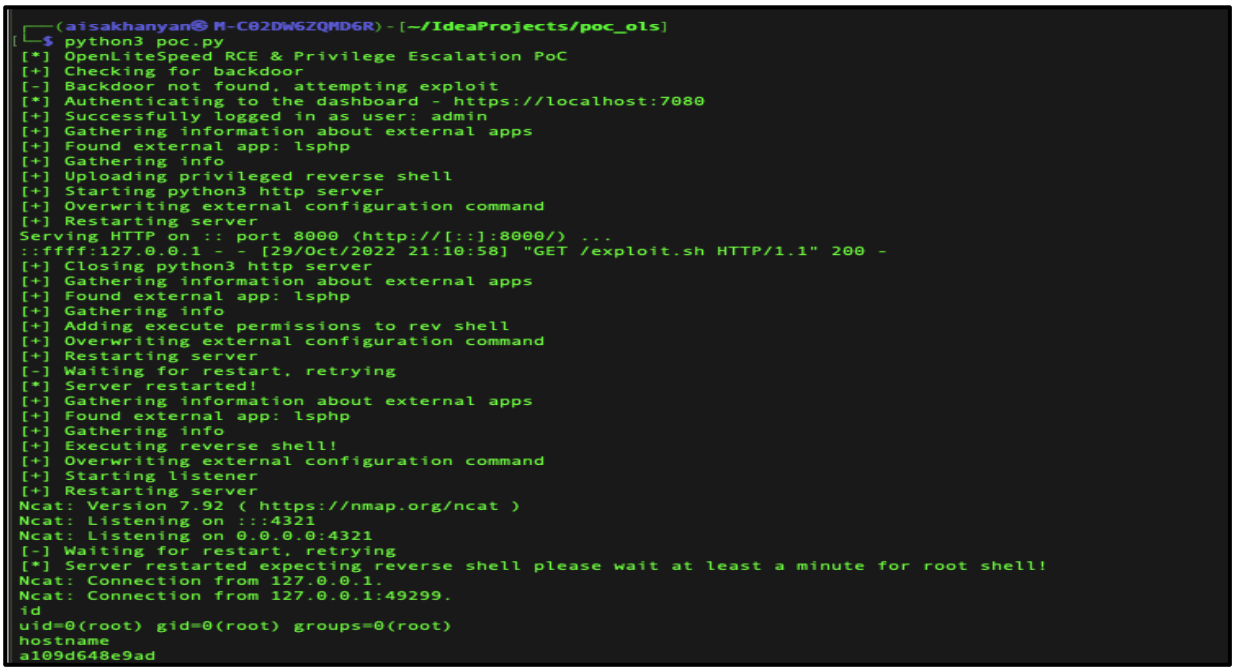
Las vulnerabilidades descubiertas son:

- Ejecución remota de código (CVE-2022-0073), clasificado como de gravedad alta (CVSS 8.8): Un atacante que lograra obtener las credenciales del dashboard podría aprovechar la vulnerabilidad para ejecutar código en el servidor.

- Escalada de privilegios (CVE-2022-0074), clasificación de gravedad alta (CVSS 8.8): una configuración incorrecta en la variable de entorno PATH podría aprovecharse para escalar privilegios.

- Recorrido de directorio (CVE-2022-0072), clasificación de gravedad media (CVSS 5.8): la explotación de esta vulnerabilidad permite a los atacantes acceder a cualquier archivo en el directorio raíz web.





Unit 42 informo de manera responsable las vulnerabilidades a LiteSpeed Technologies con una solución sugerida el 4 de octubre de 2022. LiteSpeed Technologies lanzó una versión de parche v1.7.16.1 para OpenLiteSpeed y 6.0.12 para LiteSpeed, que aborda las vulnerabilidades reveladas.

RECOMENDACIONES:

- Actualizar los firewalls con los parches adecuados para mitigar y contrarrestar estas vulnerabilidades,
- Es esencial que instales lo antes posible las actualizaciones proporcionadas por los fabricantes para cerrar posibles brechas de seguridad.

Fuentes de información	▪ hxxps://unit42.paloaltonetworks.com/openlitespeed-vulnerabilities/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 310	Fecha: 15-11-2022
		Página 8 de 13

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Vulnerabilidad crítica de escalada de privilegios locales en el Kernel de Linux.		
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		

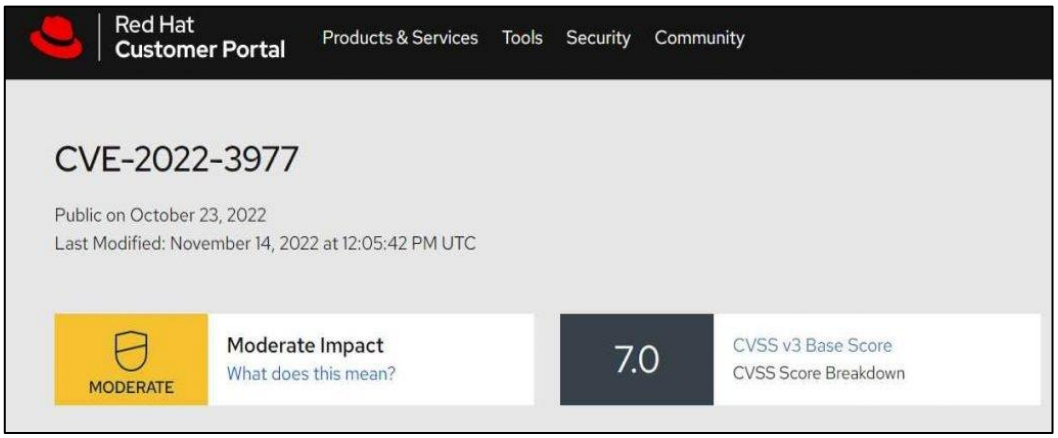
Descripción

FECHA DEL EVENTO:

El 14 de noviembre del 2022, mediante la pagina "www.securitynewspaper.com" se tomo conocimiento sobre la vulnerabilidad de escalamiento de privilegios locales en el Kernel de Linux, identificada como CVE-2022-3977 (use-after-free).

ANTECEDENTES

Esta falla se encontró después de la liberación de la funcionalidad MCTP (Protocolo de Transporte de Componentes de Administración) llamada "mctp sk unhash" que se puede explotar para elevar los privilegios a la raíz del kernel de Linux.



DETALLES:

Use-after-free se refiere a una vulnerabilidad de corrupción de memoria que ocurre cuando una aplicación intenta usar la memoria que ya no tiene asignada (o liberada), después de que esa memoria se haya asignado a otra aplicación.

La vulnerabilidad "use-after-free" se identifico dentro de "mctp_sk_unhash" en "net/mctp/af_mctp.c" en el último kernel de Linux que se puede explotar para lograr una escalada de privilegios a la raíz.

Esto puede provocar bloqueos y que los datos se sobrescriban sin darse cuenta, conducir a la ejecución de código arbitrario o permitir que un atacante obtenga capacidades de ejecución remota de código.

Actualmente, los mantenedores del kernel de Linux han lanzado formalmente correcciones de seguridad para la vulnerabilidad CVE-2022-3977.

RECOMENDACIÓN

- Se recomienda actualizar los servidores Linux de inmediato e instalar las correcciones de otras distribuciones.

Fuentes de información	▪ hxxps://www.securitynewspaper.com/2022/11/14/critical-local-privilege-escalation-vulnerability-in-linux-kernel-patch-immediately/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 310	Fecha: 15-11-2022
		Página 9 de 13

Componente que reporta	**COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ**		
Nombre de la alerta	Nuevos hashes maliciosos		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C03
Clasificación temática familia	Código malicioso		

Descripción

1. El día 15 de noviembre del 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectaron nuevas firmas de hash maliciosas, entre ellas:

ITEM	HASH SHA256	TIPO DE ARCHIVO	NOMBRE DEL ARCHIVO
1	a1be064e3cc35f968df7a27e0a928b6fc6519926eda417222ad637eb1f0d0396	exe	R22SI005577.exe
2	10b7d48bfed687e95bd78b8eeccadbf4549b37830da02211798af979d6ad1fcd	javascript	Wikipedia_pm.js
3	1dc9a71998f124f5a7d32b4a8bbadda01c4dad2029325112271216e53cb964ae	rar	SOLICITUD DE COTIZACIÓN 1307-RFQ.pdf.bz
4	db1affa56bc0685149694349d7adbf5a203b148fba4815f694d3d0912742a68f	exe	PO52652-03351007.exe
5	4db665c4d103ea1906f34ebf86c1f79494731010dc191bacbda57b16bfc8249c	zip	galafighters.zip
6	e65fab53aa77021b9bd6cf411bca12d13600f2f86d6e549f02a3d256e90600a4	exe	Galafighters.exe
7	bb2ece696d74f1251bae1e1c7282346b7ec102af84aa639b7aa9009204fca134	zip	No Determinado
8	14b0c3d3da7d6fbc9403e90a300f7ffaf737d1526cfa462180bb86d5130d2c19	zip	No Determinado
9	7f97d40af1ec95977e0ab9a4c3afb8af2bd967158b6924f7f76320e80cd24267	zip	installer.zip
10	b91e8d68481d4c5ce3ce32588278650d71ee84d7bfdd06f42393350356bfbd0d	zip	No Determinado
11	d3ac70c5df732ce13b7350851473561e765de27964c1da2eae7a7d82ea0abf03	zip	No Determinado
12	2ef9e502397e934f969647165892b6acbed805bd0b9589fdb73edfeed716c2a6	rar	JUSTIFICANTE DE PAGO.rar
13	899d0f9e8343dab899e302fa6bda0ec1bc4133f00fbb6d9215eea4b79ccf4ecb	exe	111A.exe

2. Recomendaciones:

- Evitar descargar archivos y/o enlaces de dudosa procedencia.
- Mantener los equipos protegidos, con el software actualizado.

Fuentes de información	▪ Comandancia de Ciberdefensa de la Marina, Osint

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 310**	**Fecha: 15-11-2022**
		Página 10 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Cisco Identity Services Engine		
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:**

Cisco ha reportado dos vulnerabilidades de severidad ALTA de tipo uso incorrecto de API privilegiadas y neutralización incorrecta de la entrada durante la generación de la página web (Cross-site Scripting) que afecta a Cisco Identity Services Engine (ISE). La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto autenticado omitir la autorización, obtener acceso a información confidencial y ejecutar código de secuencia de comandos arbitrario en el contexto de la interfaz afectada o acceder a información confidencial basada en el navegador.

2. **Detalles:**

- La vulnerabilidad de severidad **alta** identificada como CVE-2022-20956 en la interfaz de administración basada en web de Cisco ISE, podría permitir a un atacante remoto autenticado omitir la autorización y acceder a los archivos del sistema. Esta vulnerabilidad se debe a un control de acceso inadecuado en la interfaz de administración basada en web de un dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP manipulada al dispositivo afectado. Una explotación exitosa podría permitir que el atacante enumere, descargue y elimine ciertos archivos a los que no debería tener acceso.

  La vulnerabilidad de tipo uso incorrecto de API privilegiadas, se debe a que la aplicación no cumple con los requisitos de la API para una llamada de función que requiere privilegios adicionales. Esto podría permitir que los atacantes obtengan privilegios al hacer que la función se llame incorrectamente.

- La vulnerabilidad de severidad **media** identificada como CVE-2022-20959 en la API de servicios RESTful externos (ERS) del software Cisco ISE, podría permitir a un atacante remoto autenticado realizar un ataque de secuencias de comandos entre sitios (XSS) contra un usuario de la interfaz de un dispositivo afectado. Esta vulnerabilidad se debe a una validación de entrada insuficiente. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un administrador autenticado de la interfaz de administración basada en web para que haga clic en un enlace malicioso. Una explotación exitosa podría permitir que el atacante ejecute un código de secuencia de comandos arbitrario en el contexto de la interfaz afectada o acceda a información confidencial basada en el navegador.

  La vulnerabilidad de tipo Cross-site Scripting, se debe a que el software no neutraliza o neutraliza incorrectamente la entrada controlable por el usuario antes de que se coloque en la salida que se usa como una página web que se sirve a otros usuarios.

3. **Productos afectados:**

- La vulnerabilidad CVE-2022-20956 afecta al software Cisco ISE versión 3.1 y 3.2;
- La vulnerabilidad CVE-2022-20959 afecta al software Cisco ISE si ERS está habilitado.

4. Solución:

- Se recomienda actualizar Cisco ISE versión 3.1 a la 3.1P4 y la versión 3.2 a la 3.2P1 que corrigen estas vulnerabilidades. Asimismo, Cisco indicó que los parches activos pueden estar disponibles a pedido para ciertas versiones y niveles de parches;
- Para la vulnerabilidad CVE-2022-20959, se recomienda desactivar la función ERS.

Fuentes de información	▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx ▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-twLnpy3M

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 310**	**Fecha: 15-11-2022**
		Página 12 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en GT SoftGOT2000 de Mitsubishi Electric 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:**

   Se ha reportado una vulnerabilidad de severidad CRÍTICA de tipo inyección de comando de sistema operativo de OpenSSL conocida que afecta a GT SoftGOT2000 de Mitsubishi Electric Corporation. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar comandos maliciosos del sistema operativo.

2. **Detalles:**

   - La vulnerabilidad de severidad **crítica** identificada como CVE-2022-2068 de inyección de comando de sistema operativo en OpenSSL afecta a Mitsubishi Electric GT SoftGOT2000. Si un atacante envía un certificado especialmente diseñado, esta vulnerabilidad podría permitirle ejecutar comandos maliciosos del sistema operativo.
   - La vulnerabilidad de tipo Inyección de comando de sistema operativo se debe a que el software construye la totalidad o parte de un comando del sistema operativo utilizando la entrada influenciada externamente desde un componente ascendente, pero no neutraliza o neutraliza incorrectamente los elementos especiales que podrían modificar el comando previsto del sistema operativo cuando se envía a un componente descendente.

3. **Productos afectados:**

   - Mitsubishi Electric informa que esta vulnerabilidad afecta a OpenSSL en los siguientes productos: GT SoftGOT2000 1.275M—1.280S.

4. **Solución:**

   - Mitsubishi Electric recomienda instalar la versión 1.285X o posterior para mitigar esta vulnerabilidad. Así como tomar las siguientes medidas de mitigación para minimizar el riesgo de explotación de esta vulnerabilidad:
     - Utilizar los productos afectados desde dentro de una red de área local (LAN) y bloquear el acceso desde redes y hosts que no sean de confianza;
     - Instalar el software antivirus en la máquina host donde están instalados los productos afectados;
     - Restringir el acceso físico a la máquina host con los productos instalados y el equipo de red;
     - No almacenar certificados que no sean de confianza;
     - No hacer clic en enlaces web en correos electrónicos o cualquier otra comunicación de fuentes no confiables.

Fuentes de información	▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-319-01

Índice alfabético

acceder 6
acceso a la información 4
actualización de noviembre 4
atacante remoto 10
Cisco 10
clave PIN 4
código PUK 4
comandos 10
corrupción de memoria 8
Cross-site Scripting 10
CVE-2022-0072 6
CVE-2022-0073 6
CVE-2022-0074 6
CVE-2022-20465 4
CVE-2022-2068 12
CVE-2022-20956 10
CVE-2022-20959 10
CVE-2022-3977 8
dashboard 6
desbloquear 4
dispositivos Android 4
ejecución remota 6
escalar privilegios 6
explotación 12
Google 4
GT SoftGOT2000 12
hash maliciosas 9
información confidencial 10
Kernel de Linux 8
LiteSpeed 6
MCTP 8
OpenLiteSpeed 6
página web 10
severidad 12
sistema operativo 12
tarjeta SIM 4
use-after-free 8
vulnerabilidad 12
vulnerabilidades 6