GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3025

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	2	1	0
MALWARE	1	0	0
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

VULNERABILIDADES RCE NO AUTENTICADAS EN CISCO IDENTITY SERVICES ENGINE (ISE / ISE-PIC)

Cisco ha publicado actualizaciones críticas para corregir múltiples vulnerabilidades de ejecución remota de código (RCE), identificadas como CVE-2025-20281, CVE-2025-20282 y CVE-2025-20337, que permiten a un atacante remoto y sin credenciales tomar el control total del sistema operativo subyacente en instancias de Cisco ISE o ISE-PIC, con privilegios de root.

Resumen técnico:

- CVE-2025-20281 y CVE-2025-20337 (CVSS 10.0):
  Se explotan mediante solicitudes API manipuladas que no validan adecuadamente los datos de entrada.

- CVE-2025-20282 (CVSS 10.0):
  Presente únicamente en Cisco ISE 3.4.
  Permite la carga y ejecución de archivos maliciosos en directorios privilegiados del sistema debido a la ausencia de validaciones durante el manejo de archivos en una API interna.

Estas vulnerabilidades son independientes entre sí y no requieren explotación conjunta. Cisco confirmó intentos de explotación activa de las fallas CVE-2025-20281 y CVE-2025-20337 en julio de 2025.

Impacto potencial:

- Compromiso completo del sistema operativo subyacente con privilegios de root.
- Riesgo crítico para la infraestructura de control de acceso, integración con Active Directory y tráfico sensible (VPN, VLAN, etc.).
- Explotación sin necesidad de credenciales válidas o interacción del usuario.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a las versiones corregidas recomendadas por Cisco:
   - ISE 3.3: actualizar a Patch 7
   - ISE 3.4: actualizar a Patch 2
   - Las versiones 3.2 y anteriores no se ven afectadas.
2. Evitar el uso de hot patches intermedios, ya que no mitigan completamente todas las vulnerabilidades.
3. Aplicar segmentación estricta de red para limitar el acceso a APIs de administración.
4. Monitorear logs de API y eventos anómalos en Cisco ISE.

Prioridad: Critica.

Ampliar Información:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6
- https://nvd.nist.gov/vuln/detail/CVE-2025-20281

- https://arcticwolf.com/resources/blog/cve-2025-20281-cve-2025-20282/
- https://www.cve.org/CVERecord?id=CVE-2025-20281
- https://thehackernews.com/2025/07/cisco-confirms-active-exploits.html
- https://securityaffairs.com/180044/security/cisco-patches-critical-cve-2025-20337-bug-in-identity-services-engine-with-cvss-10-severity.html

CISCO IOS / IOS XE — VULNERABILIDADES DE EJECUCIÓN REMOTA DE CÓDIGO (RCE) A TRAVÉS DE SNMP EN EL SOFTWARE CISCO IOS E IOS XE

Cisco ha actualizado su aviso de seguridad para abordar múltiples vulnerabilidades críticas que afectan dispositivos que ejecutan Cisco IOS e IOS XE con SNMP habilitado, permitiendo a un atacante remoto ejecutar código o forzar reinicios del sistema mediante paquetes SNMP manipulados.

Resumen técnico:

- CVE-2017-6736, CVE-2017-6737, CVE-2017-6738, y otros (CVSS 8.8): Estas vulnerabilidades se deben a condiciones de desbordamiento de búfer en el subsistema SNMP, afectando las versiones 1, 2c y 3 del protocolo.
  En SNMP v2c o anterior, el atacante debe conocer la cadena de comunidad SNMP.
  En SNMP v3, requiere credenciales válidas.
- El envío de paquetes SNMP especialmente diseñados puede provocar la ejecución remota de comandos o la recarga del dispositivo, comprometiendo routers, switches y otros equipos empresariales.

Impacto potencial:

- Ejecución remota de código arbitrario con privilegios totales.
- Reinicio forzado del sistema afectado, causando interrupción de servicios.
- Exposición de infraestructura crítica si SNMP está accesible desde redes no confiables.

Recomendaciones de mitigación:

1. Actualizar inmediatamente los dispositivos afectados usando el Cisco IOS Software Checker.
2. Aplicar restricciones SNMP:
    - Limitar acceso a administradores autorizados.
    - Bloquear tráfico SNMP desde redes externas.
3. Deshabilitar MIBs afectados mediante snmp-server view, siguiendo la guía oficial del aviso.
4. Auditar actividad SNMP y logs de sistema, prestando atención a reinicios inesperados o archivos crashinfo.

Prioridad: Urgente.

Ampliar Información:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp
- https://www.zerodayinitiative.com/advisories/ZDI-25-279/

TP-LINK VIGI NVR – EJECUCIÓN DE COMANDOS REMOTOS (CVE-2025-7723 / CVE-2025-7724)

El 25 de julio de 2025, TP-Link publicó parches para dos vulnerabilidades críticas que afectan a sus videograbadores de red (NVR) VIGI NVR1104H-4P V1 y VIGI NVR2016H-16MP V2. Una de ellas permite ejecución remota de comandos sin autenticación desde la red local, comprometiendo completamente el dispositivo.

Resumen técnico:

- CVE: CVE-2025-7723 y CVE-2025-7724 — Vector: Red local, baja complejidad.
  Detalles: CVE-2025-7723 permite que un usuario autenticado ejecute comandos del sistema operativo como root a través de inyecciones en las peticiones CGI del panel de administración.

CVE-2025-7724 puede ser explotada sin necesidad de credenciales, permitiendo el compromiso total del videograbador desde la red local.

Ambas fallas permiten la ejecución remota de comandos, modificación o eliminación de grabaciones y uso del dispositivo como pivote para atacar otros equipos de la red.

Versiones afectadas:

- VIGI NVR1104H-4P V1 con firmware anterior a 1.1.5 Build 250518
- VIGI NVR2016H-16MP V2 con firmware anterior a 1.3.1 Build 250407

Impacto potencial:

- Acceso root remoto al NVR.
- Secuestro de cámaras IP, manipulación de grabaciones.
- Movimiento lateral dentro de la red (pivoting).
- Ejecución de malware, integración en botnets IoT, o minería de criptomonedas.

Recomendaciones de mitigación:

- Actualizar firmware inmediatamente a las versiones seguras:
  - NVR1104H-4P V1 → 1.1.5 Build 250518.
  - NVR2016H-16MP V2 → 1.3.1 Build 250407.
- Revocar credenciales tras el parche y cerrar sesiones activas.
- Limitar el acceso al puerto de administración por ACL o VPN.
- Deshabilitar servicios innecesarios como Telnet, FTP o UPnP.
- Monitorizar logs por comandos sospechosos.

Prioridad: Critica.

Ampliar Información:

- https://unaaldia.hispasec.com/2025/07/tp-link-corrige-dos-vulnerabilidades-criticas-en-videograbadores-vigi-que-permiten-ejecutar-comandos-remotos.html
- https://cyberpress.org/tp-link-network-video-recorder-vulnerability/
- https://nvd.nist.gov/vuln/detail/CVE-2025-7724

Recomendaciones Generales Sobre Vulnerabilidades:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves.

1. Aplicar las actualizaciones de seguridad proporcionadas por Microsoft para las versiones afectadas de Windows Serve
2. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.
3. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.
4. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.
5. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.
6. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

PLATAFORMA DE PHISHING COMO SERVICIO "DARCULA SUITE 3.0" AUTOMATIZA ATAQUES PERSONALIZADOS

La plataforma Darcula PhaaS (Phishing-as-a-Service) ha lanzado su versión 3.0, denominada Darcula Suite, la cual permite generar automáticamente kits de phishing personalizados dirigidos a cualquier marca, reduciendo drásticamente la barrera de entrada para atacantes novatos.

Resumen técnico:

- Generador automático de kits de phishing: solo se necesita ingresar la URL de la marca objetivo. El sistema clona el sitio real (HTML, CSS, JS) utilizando Puppeteer, permitiendo modificar formularios, campos de inicio de sesión, 2FA y más.
- Paquete de ataque: el sitio finalizado se empaqueta en un archivo .cat-page, se sube al panel de administración de Darcula y queda listo para ser desplegado.
- Panel de control:
  - Seguimiento de campañas.
  - Registro en tiempo real de credenciales robadas.
  - Notificaciones por Telegram.
  - Conversión de tarjetas robadas a imágenes virtuales para apps de pago.

- Funciones avanzadas:
  - Filtro de IP y bots.
  - Bloqueo de rastreadores.
  - Segmentación por tipo de dispositivo.

- Disponibilidad: se han detectado contenedores públicos del sistema, lo que ha permitido estimar un aumento significativo en el número de operadores activos antes del lanzamiento oficial.

Impacto potencial:

- Aumento masivo de campañas de phishing dirigidas a cualquier marca, sin necesidad de conocimientos técnicos.
- Dificultad para detección y respuesta temprana, por el uso de técnicas antidetección automatizadas.
- Amenaza en evolución, impulsada por modelos de negocio tipo cibercrimen como servicio.

Recomendaciones de mitigación:

1. Capacitar al personal frente a sitios clonados y phishing altamente convincente.
2. Implementar soluciones anti-phishing con detección por comportamiento y sandboxing.
3. Monitorear accesos anómalos desde dominios desconocidos o servicios de URL acortados.
4. Utilizar autenticación multifactor robusta, preferiblemente sin SMS.

Prioridad: Crítica.

Ampliar Información:

- https://blog.segu-info.com.ar/2025/07/darcula-phaas-30-genera-automaticamente.html
- https://www.helpnetsecurity.com/2025/02/20/darcula-allows-tech-illiterate-crooks-to-create-deploy-diy-phishing-kits-targeting-any-brand/
- https://www.darkreading.com/threat-intelligence/darcula-phishing-kit-impersonate-brand
- https://www.netcraft.com/blog/darcula-v3-phishing-kits-targeting-any-brand

Recomendaciones generales sobre malware:

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

CAMPAÑA DE EXTORSIÓN MASIVA CONTRA CLIENTES DE SALESFORCE LIGADA AL GRUPO SHINYHUNTERS

El grupo de ciberextorsión ShinyHunters ha sido vinculado a múltiples violaciones de datos dirigidas a instancias de Salesforce CRM pertenecientes a grandes empresas como Qantas, Allianz Life, LVMH, Dior, Louis Vuitton, Tiffany & Co. y Adidas.
Resumen técnico

- La campaña se basa en ataques de ingeniería social avanzada (voice phishing o vishing), donde los atacantes se hacen pasar por personal de soporte técnico para engañar a empleados y lograr que conecten aplicaciones maliciosas a sus cuentas de Salesforce.
- La técnica consiste en inducir a la víctima a introducir un “código de conexión” en la configuración de apps conectadas de Salesforce, lo que permite a los atacantes insertar una versión maliciosa del Data Loader OAuth app (a veces disfrazado como "My Ticket Portal").
- Además del vishing, algunos accesos se lograron a través de phishing tradicional con páginas falsas de inicio de sesión de Okta, robando credenciales y tokens MFA.
- Las tablas afectadas fueron principalmente "Accounts" y "Contacts", revelando acceso a datos sensibles de clientes.

Impacto potencial

- Aunque aún no se han filtrado los datos públicamente, los atacantes están enviando correos de extorsión privada a las empresas, identificándose como ShinyHunters.
- Se cree que, en caso de no recibir pagos, liberarán gradualmente los datos robados, como hicieron anteriormente en los ataques a Snowflake, Oracle Cloud, AT&T, Wattpad y NitroPDF.

- Existe fuerte evidencia de que ShinyHunters y Scattered Spider (UNC3944) comparten miembros y técnicas, lo que dificulta la atribución directa de los ataques.

Recomendaciones para mitigar el riesgo:

- Salesforce no fue comprometido, pero los clientes deben reforzar medidas de seguridad.
- Habilitar MFA obligatoria en todas las cuentas.
- Limitar aplicaciones conectadas a IP confiables.
- Aplicar el principio de mínimos privilegios para apps OAuth.
- Usar Salesforce Shield para monitoreo de eventos y políticas transaccionales.
- Registrar un Security Contact para respuesta ante incidentes.

Prioridad: Importante.

Ampliar Información:

- https://www.bleepingcomputer.com/news/security/shinyhunters-behind-salesforce-data-theft-attacks-at-qantas-allianz-life-and-lvmh/
- https://www.bankinfosecurity.com/allianz-life-breach-tied-to-crm-compromise-a-29068
- https://www.ampcuscyber.com/shadowopsintel/customer-records-compromised-in-allianz-life-breach/