GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4625

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
VULNERABILIDADES	3	0	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

CVE-2025-20333, CVE-2025-20362 Y CVE-2025-20363 — CISCO SECURE FIREWALL ASA, FTD, IOS, IOS XE E IOS XR — EJECUCIÓN REMOTA DE CÓDIGO Y DENEGACIÓN DE SERVICIO

Cisco alertó sobre una nueva variante de ataques activos dirigida a los dispositivos Secure Firewall ASA y Firepower Threat Defense (FTD), explotando las vulnerabilidades CVE-2025-20333 y CVE-2025-20362, además de una tercera falla crítica CVE-2025-20363 que amplía el vector de ataque a Cisco IOS, IOS XE e IOS XR.

Los ataques, atribuidos al grupo ArcaneDoor, permiten la ejecución remota de código (RCE) y la omisión de autenticación en servicios web de los firewalls, generando reinicios inesperados (DoS) y comprometiendo completamente los dispositivos afectados.

Resumen técnico:

- CVE-2025-20333 (CVSS 9.9): falla en el VPN Web Server por validación inadecuada de entradas HTTP(S), explotable por un usuario VPN autenticado. Permite ejecutar código arbitrario como root.
- CVE-2025-20362: vulnerabilidad de autorización insuficiente que posibilita el acceso a URLs restringidas sin autenticación previa.
- CVE-2025-20363 (CVSS 9.0): vulnerabilidad en los servicios web de Cisco ASA, FTD, IOS, IOS XE e IOS XR, explotable por atacantes remotos no autenticados (ASA/FTD) o autenticados con bajos privilegios (IOS/IOS XE/XR). Permite ejecución de código como root.
- Las tres vulnerabilidades se relacionan con ataques activos desde mayo de 2025, en los que se desplegaron malware personalizados como RayInitiator y LINE VIPER, usados para persistencia en hardware Cisco ASA 5500-X.
- No existen workarounds efectivos. Cisco recomienda aplicar actualizaciones inmediatas a las versiones corregidas.

Impacto potencial:

- Ejecución remota de código (RCE) en múltiples plataformas de Cisco.
- Denegación de servicio (DoS) por reinicios continuos de dispositivos vulnerables.
- Compromiso total del firewall o router afectado, incluyendo exfiltración de tráfico, manipulación de logs y persistencia avanzada.
- Posible movimiento lateral hacia redes internas a través de dispositivos comprometidos.
- Afecta entornos críticos de telecomunicaciones, gobierno y defensa.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a los firmwares corregidos indicados en los avisos de seguridad de Cisco.
2. Verificar si los servicios SSL VPN o WebVPN están habilitados mediante el comando *show running-config* y desactivarlos si no son necesarios.
3. Revisar configuraciones de acceso remoto en FMC/FDM para deshabilitar funciones no utilizadas.
4. Implementar monitoreo continuo de tráfico y alertas ante reinicios o comportamientos anómalos.
5. Revisar integridad del ROM Monitor (ROMmon) para detectar posibles modificaciones.
6. Aplicar segmentación de red y limitar el acceso administrativo desde redes no seguras.

Prioridad: Crítica.

Ampliar información:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h3O
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB
- https://securityaffairs.com/184290/security/cisco-became-aware-of-a-new-attack-variant-against-secure-firewall-asa-and-ftd-devices.html
- https://thehackernews.com/2025/11/cisco-warns-of-new-firewall-attack.html

CVE-2025-12480 — GLADINET TRIOFOX — BYPASS DE AUTENTICACIÓN Y EJECUCIÓN REMOTA DE CÓDIGO

Una vulnerabilidad crítica en la plataforma de compartición y acceso remoto Gladinet Triofox permite a atacantes no autenticados acceder a las páginas de configuración inicial del sistema incluso después de completada la instalación, posibilitando la creación de cuentas administrativas y la ejecución de código arbitrario con privilegios de sistema.

Resumen técnico:

- Identificada como CVE-2025-12480 con una puntuación CVSS 9.1 (Crítica).
- Clasificada como una falla de Improper Access Control (CWE-284), explotable sin autenticación previa.
- El actor de amenazas UNC6485 (vinculado a campañas activas desde agosto de 2025) explotó la vulnerabilidad para acceder a las páginas de configuración restringidas.
- El ataque se basa en la manipulación del encabezado HTTP Host, que permite suplantar la dirección localhost y ejecutar nuevamente el proceso de configuración.
- Esto posibilita la creación de una nueva cuenta administrativa local denominada “Cluster Admin”, utilizada para subir archivos y ejecutar código.
- Se abusa de la función antivirus integrada, que permite definir rutas personalizadas, para ejecutar scripts maliciosos con privilegios SYSTEM.
- Los atacantes desplegaron herramientas legítimas como Zoho Assist, AnyDesk, Plink y PuTTY para establecer túneles cifrados y mantener persistencia remota.
- Afecta versiones anteriores a 16.7.10368.56560, parcheada en julio de 2025.

Impacto potencial:

- Compromiso total del sistema afectado, con posibilidad de ejecución remota de código y control administrativo completo.
- Riesgo de movimiento lateral, robo de credenciales y persistencia mediante herramientas legítimas.
- Afecta directamente la confidencialidad, integridad y disponibilidad del entorno comprometido.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a Triofox v16.7.10368.56560 o superior.
2. Auditar todas las cuentas administrativas y eliminar usuarios no autorizados ("Cluster Admin").
3. Revisar la configuración del motor antivirus y bloquear rutas personalizadas que apunten a scripts o binarios.
4. Monitorizar conexiones SSH salientes inusuales (puerto 433) y validar la integridad de los componentes del sistema.

Prioridad: Crítica.

Ampliar información:

- https://socprime.com/blog/cve-2025-12480-detection/
- https://socradar.io/labs/app/cve-radar/cve-2025-12480
- https://www.infosecurity-magazine.com/news/hackers-exploit-critical-flaw/
- https://www.techradar.com/pro/security/hackers-hijack-antivirus-features-to-install-malware-heres-what-we-know
- https://thehackernews.com/2025/11/hackers-exploiting-triofox-flaw-to.html

MÚLTIPLES VULNERABILIDADES CRÍTICAS EN MICROSOFT WINDOWS — PATCH TUESDAY NOVIEMBRE 2025

Microsoft liberó actualizaciones de seguridad para 63 vulnerabilidades identificadas en sus productos, entre ellas cuatro catalogadas como críticas y una bajo explotación activa en entornos reales (zero-day).

El conjunto de fallas impacta componentes como Windows Kernel, GDI+, Kerberos, Office y Visual Studio, abarcando vulnerabilidades de ejecución remota de código (RCE), elevación de privilegios (LPE), divulgación de información, denegación de servicio (DoS) y bypass de características de seguridad.

Resumen técnico:

- Microsoft publicó actualizaciones de seguridad correspondientes a noviembre de 2025, corrigiendo 63 vulnerabilidades en diversos productos del ecosistema Windows, Office, .NET y Visual Studio.
- Entre ellas destaca una vulnerabilidad zero-day activamente explotada (CVE-2025-62215) en el Windows Kernel, que permite la elevación de privilegios locales hasta nivel SYSTEM, aprovechando una condición de carrera en la gestión de recursos compartidos.
- Se abordaron además vulnerabilidades críticas de ejecución remota de código (RCE), como CVE-2025-60724 (GDI+) y CVE-2025-62199 (Microsoft Office), con puntuaciones CVSS superiores a 9.0, que permitirían la ejecución de código arbitrario en sistemas afectados.
- En total, se incluyen 29 fallas de escalada de privilegios, 16 de ejecución remota de código, 11 de divulgación de información, y otros errores de denegación de servicio, spoofing y bypass de seguridad.
- La explotación de estas vulnerabilidades podría combinarse para comprometer completamente un entorno Windows mediante cadenas de ataque que inicien con RCE y culminen con escalación de privilegios.

Impacto potencial:

- Compromiso completo de sistemas Windows mediante ejecución arbitraria de código.
- Escalada de privilegios locales hasta nivel SYSTEM, permitiendo control total del dispositivo.
- Acceso no autorizado a información sensible o credenciales del dominio.
- Posible movimiento lateral dentro de redes corporativas.
- Riesgo de implantación de malware o ransomware en entornos no parcheados.

Recomendaciones de mitigación:

1. Aplicar de forma inmediata los parches correspondientes al Microsoft Patch Tuesday de noviembre 2025, priorizando CVE-2025-62215, CVE-2025-60724 y CVE-2025-62199.
2. Implementar políticas de gestión de vulnerabilidades y pruebas post-parcheo para validar la corrección efectiva.
3. Revisar permisos de usuario y privilegios locales, minimizando cuentas con acceso administrativo.
4. Asegurar la actualización de productos dependientes como Office, Visual Studio y servicios en la nube de Microsoft.
5. Mantener una estrategia de monitoreo continuo y detección de explotación activa, especialmente ante vulnerabilidades de kernel.

+

Prioridad: Crítica.

Ampliar información:

- https://www.helpnetsecurity.com/2025/11/12/patch-tuesday-microsoft-cve-2025-62215/
- https://blog.qualys.com/vulnerabilities-threat-research/2025/11/11/microsoft-patch-tuesday-november-2025-security-update-review
- https://thehackernews.com/2025/11/microsoft-fixes-63-security-flaws.html
- https://www.wiz.io/vulnerability-database/cve/cve-2025-60724

MALWARE

GOOTLOADER — CARGADOR DE MALWARE BASADO EN JAVASCRIPT

GootLoader es un cargador de malware escrito en JavaScript, activo desde hace varios años y empleado como vector inicial de ataque en campañas de ransomware y espionaje. Se propaga mediante sitios web comprometidos y técnicas de envenenamiento SEO, haciéndose pasar por descargas legítimas de documentos o plantillas legales. Una vez ejecutado, instala componentes adicionales como backdoors, herramientas de acceso remoto o ransomware, facilitando el compromiso total de la red corporativa.

Resumen técnico:

- El malware resurgió a finales de octubre de 2025 tras varios meses de inactividad, introduciendo nuevas tácticas de evasión avanzada y ofuscación visual.
- Utiliza fuentes web personalizadas (WOFF2) con sustitución de glifos para ocultar nombres de archivos maliciosos dentro del código HTML, evadiendo herramientas de análisis.

- Distribuye archivos ZIP malformados que muestran contenido inofensivo en entornos de análisis, pero que en sistemas Windows extraen scripts JavaScript maliciosos (.js).
- Al ejecutarse, el malware descarga e instala Supper (SocksShell), una puerta trasera con capacidad SOCKS5 y control remoto.
- Permite movimiento lateral, creación de cuentas administrativas y persistencia en el entorno comprometido.
- Las infecciones recientes fueron atribuidas a los grupos Hive0127 / Storm-0494, que ceden acceso a Vanilla Tempest y Vice Society para desplegar ransomware INC.

Impacto potencial:

- Compromiso completo de estaciones Windows y controladores de dominio.
- Acceso remoto a la infraestructura mediante backdoors persistentes.
- Despliegue de ransomware y robo de credenciales.
- Evasión de defensas tradicionales (AV/EDR) mediante fuentes personalizadas y manipulación de archivos ZIP.
- Riesgo elevado para entornos con WordPress vulnerables o mal configurados.

Recomendaciones de mitigación:

1. Evitar la descarga de documentos o plantillas desde sitios no verificados o desconocidos.
2. Actualizar WordPress y sus complementos, eliminando plugins obsoletos o inseguros.
3. Monitorear actividad anómala en navegadores y PowerShell, así como nuevas cuentas de usuario no autorizadas.
4. Revisar tráfico de red en busca de conexiones proxy (SOCKS5) o comportamientos sospechosos.
5. Mantener EDR y antivirus actualizados con firmas recientes de GootLoader y Supper.

6. Aplicar segmentación de red y controles de acceso para limitar el movimiento lateral.

Prioridad: Urgente.

Ampliar información:

- https://blog.tecnetone.com/gootloader-vuelve-el-malware-regresa-con-nuevas-tacticas-en-2025
- https://cisoseries.com/cybersecurity-news-googles-remote-wipe-weapon-qilin-ransomware-activity-surges-gootloader-is-back/
- https://www.ciberplaneta.org/articles/341/
- https://www.techradar.com/pro/security/gootloader-strikes-again-using-font-hack-to-spread-malware-on-wordpress-sites
- https://thehackernews.com/2025/11/gootloader-is-back-using-new-font-trick.html

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

GOOGLE DEMANDA A HACKERS CHINOS DETRÁS DE LA PLATAFORMA LIGHTHOUSE — PHISHING-AS-A-SERVICE DE MIL MILLONES DE DÓLARES.

Google presentó una demanda civil en el Tribunal del Distrito Sur de Nueva York (SDNY) contra un grupo de ciberdelincuentes con sede en China, responsables de operar "Lighthouse", una plataforma de Phishing-as-a-Service (PhaaS) utilizada para lanzar campañas masivas de smishing (phishing por SMS).

Según Google, el grupo ha comprometido más de un millón de víctimas en 120 países y generado más de mil millones de dólares en ganancias ilícitas a lo largo de tres años, utilizando marcas reconocidas como Google, USPS y E-ZPass para engañar a usuarios y robar información financiera.

Resumen técnico:

- La plataforma Lighthouse permite a los delincuentes ejecutar campañas automatizadas de phishing y smishing, ofreciendo kits con plantillas de sitios falsos que imitan portales legítimos de empresas y gobiernos.
- Estas campañas utilizan mensajes SMS con enlaces fraudulentos que conducen a páginas de inicio de sesión falsas, diseñadas para robar credenciales, contraseñas y datos financieros.
- Google identificó al menos 107 plantillas de sitios web que usaban su marca e interfaz para engañar a las víctimas.

- La operación está asociada con el grupo “Smishing Triad”, que ha desplegado más de 194,000 dominios maliciosos desde 2024, vinculados también a plataformas similares como Lucid y Darcula.
- Los kits Lighthouse se comercializan en foros y canales de Telegram, con precios entre $88 y $1,588 USD, y ofrecen infraestructura lista para ejecutar campañas masivas.
- La compañía busca desmantelar la red bajo las leyes estadounidenses RICO (Racketeer Influenced and Corrupt Organizations), Lanham Act y Computer Fraud and Abuse Act, sentando un precedente legal contra servicios PhaaS.

Impacto potencial:

- Ampliación de ataques de phishing a escala global, con miles de dominios activos.
- Robo de datos financieros y credenciales de acceso a servicios bancarios y plataformas en línea.
- Riesgo de usurpación de identidad, fraude y pérdida económica para usuarios y empresas.
- Potencial uso de los datos robados para lavado de dinero, estafas y fraude en tarjetas de crédito.
- Incremento en la profesionalización del modelo Phishing-as-a-Service, reduciendo la barrera técnica para ciberdelincuentes.

Recomendaciones para mitigar el riesgo:

1. Evitar acceder a enlaces incluidos en mensajes SMS o correos no solicitados.
2. Verificar siempre la autenticidad de las páginas antes de ingresar credenciales o información personal.
3. Activar filtros de spam y protección contra smishing en dispositivos Android e iOS, en iPhone: activar "Filter Unknown Senders" y "Filter Junk" y En Android: habilitar Spam Protection y reportar mensajes al 7726 (SPAM).
4. Implementar autenticación multifactor (MFA) en todas las cuentas sensibles.
5. Educar a los usuarios sobre campañas de phishing actuales y técnicas de ingeniería social.
6. Las organizaciones deben monitorizar dominios falsos o abusos de marca relacionados con sus servicios.

Prioridad: Importante.

Ampliar Información:

- https://www.cnbc.com/2025/11/12/google-e-zpass-usps-text-scam-phishing-suit.html
- https://www.cbsnews.com/news/google-lawsuit-text-message-phishing-attacks/
- https://www.irishtimes.com/business/2025/11/12/google-sues-chinese-group-selling-software-behind-text-message-scams/
- https://thehackernews.com/2025/11/google-sues-china-based-hackers-behind.html