

**GammaCSOC-CERT**  
By Gamma Ingenieros



# Boletín de Ciberseguridad Semanal

Edición °2625



## 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
<b>VULNERABILIDADES</b>	2	0	0
<b>MALWARE</b>	1	0	0
<b>NOTICIAS DE CIBERSEGURIDAD</b>	0	1	0

### VULNERABILIDADES

#### **Vulnerabilidades RCE no autenticidad en Cisco Identity Services Engine (ISE / ISE-PIC)**

Cisco ha publicado actualizaciones críticas para corregir dos vulnerabilidades de ejecución de código remoto (RCE), CVE-2025-20281 y CVE-2025-20282, que permiten a un atacante remoto y sin credenciales tomar el control total del servidor ISE o ISE-PIC como root.

Resumen técnico:

- CVE-2025-20281(CVSS 10.0):

Se aprovecha por una validación insuficiente en una API interna de Cisco ISE / ISE-PIC (v. 3.3 y posterior), permitiendo enviar solicitudes maliciosas que ejecutan comandos arbitrarios como root.

- CVE-2025-20282(CVSS 10.0):

Afecta exclusivamente la versión 3.4 y se basa en la ausencia de validación al cargar archivos maliciosos en directorios privilegiados, seguido de su ejecución con acceso root.

Ambas vulnerabilidades permiten inyección de comandos o carga de malware sin necesidad de autenticarse y se aprovechan mediante peticiones API manipuladas.

Impacto potencial:

- Compromiso total de instancias ISE/I-PIC.
- Control administrativo del dispositivo, acceso al Active Directory, interceptación de tráfico VLAN/VPN inexplorado.
- Riesgo alto por sistemas ISE utilizados como controladores de acceso en redes empresariales.

Recomendaciones de mitigación:

1. Actualizar inmediatamente Cisco ISE / ISE-PIC a versiones parcheadas:
  - 3.3 y anteriores a 3.3P6: actualizar a 3.3P6 o superior.
  - 3.4 antes de 3.4P2: actualizar a 3.4P2 o superior.
2. Restricción urgente de acceso: limitar acceso API solo a redes seguras y administradores de confianza.
3. Auditoría post-parche: revisar logs y actividad de API tras la actualización para detectar anomalías.
4. Eliminar versiones vulnerables: reemplazar nodos en la nube y entornos híbridos con versiones recientes o parcheadas.

**Prioridad: Crítica.**

**Ampliar Información:**

- <https://ciberseguridad.euskadi.eus/noticia/2025/vulnerabilidades-de-ejecucion-remota-de-codigo-no-autenticado-en-cisco-identity-services-engine/webcyb00-ontcibglos/es>

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6>
- <https://beaconlab.us/es/publicacion/alerta-2025-54-vulnerabilidades-criticas-en-cisco-ise>

## **Vulnerabilidad de escalada de privilegios HPE ONEVIEW de VMWARE VCENTER (CVE-2025-37101)**

Se ha identificado una vulnerabilidad crítica en HPE OneView para VMware vCenter (OV4VC) que permite a un usuario con permisos de solo lectura escalar privilegios y ejecutar acciones administrativas.

Resumen técnico:

- CVE: CVE-2025-37101 Vector: Red, baja complejidad, requiere mínimo privilegio y mínima interacción del usuario.
- Detalles: Un usuario con rol de solo lectura puede explotar la vulnerabilidad para obtener privilegios administrativos. Esto permite modificar configuraciones, acceder a funciones de gestión y potencialmente comprometer entornos virtualizados.
- Versiones afectadas: Todas las versiones de OV4VC anteriores a la v11.7, incluyendo integración con Operations Manager y Log Insight.

Impacto potencial:

- Control administrativo total del entorno OW4VC.
- Posible manipulación, interrupción o eliminación de máquinas virtuales.
- Riesgo para infraestructura crítica de virtualización gestionada por HPE/VMware.
- Acechado por red de confianza, comprometiendo operaciones y seguridad del datacenter.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a HPE OneView for VMware vCenter v11.7.
2. Auditar cuentas de usuario, restringiendo quienes tienen acceso de solo lectura.

3. Revisar logs por actividades administrativas inesperadas.
4. Aplicar principio de mínimo privilegio: limitar usuarios con permisos elevados.
5. Monitorear y alertar sobre cambios críticos en la configuración del sistema.

**Prioridad: Crítica.**

**Ampliar Información:**

- <https://ciberseguridad.euskadi.eus/noticia/2025/vulnerabilidad-de-elevacion-de-privilegios-en-hpe-oneview-para-vmware-vcntr-ov4vc/webcyb00-contcibglos/es>
- <https://nvd.nist.gov/vuln/detail/CVE-2025-37101>
- [https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04876en\\_us&ocLocale=en\\_US](https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04876en_us&ocLocale=en_US)
- <https://www.linkedin.com/pulse/critical-hpe-security-flaw-exposes-enterprises-admin-level-febin-sani-myInc>

**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

### **Stealth Falcon (APT) explota Zero-Day en WEBDAV para desplegar malware (CVE-2025-33053)**

Investigadores de Check Point Research han confirmado que el grupo APT Stealth Falcon (también conocido como FruityArmor) explotó la vulnerabilidad CVE-2025-33053, un fallo RCE no autenticado en Windows WebDAV, durante ataques dirigidos desde marzo de 2025 a organizaciones de defensa en Turquía, Qatar, Egipto y Yemen.

#### Resumen técnico:

- CVE-2025-33053 (CVSS 8.8): Permite ejecución remota de código explotando cómo Windows maneja un archivo .url con WorkingDirectory apuntado a un recurso WebDAV malicioso.
- El archivo .url («atajo de Internet») carga iediagcmd.exe —una herramienta legítima— con la ruta de trabajo en un recurso remoto, provocando descarga y ejecución de un binario malicioso (como route.exe) desde el servidor del atacante.
- La cadena de ataque incluye la instalación de Horus Loader, seguido del implantador Horus Agent (un agente C2 avanzado basado en Mythic), junto con módulos de robo de credenciales, keylogger y backdoor persistente.

#### Impacto potencial:

- Compromiso silencioso del sistema sin necesidad de descarga visible.
- Despliegue avanzado de espionaje en infraestructura sensible.
- Instancias dirigidas en el sector defensa del Medio Oriente—alta criticidad estratégica.



Recomendaciones de mitigación:

1. Aplicar el parche oficial de junio 2025 en todos los sistemas Windows afectados, incluyendo versiones fuera de ciclo de soporte.
2. Bloquear acceso a recursos WebDAV desde entornos sensibles, incluyendo navegación atípica o lentitud en iediagcmd.exe.
3. Monitorear logs de eventos asociados a ejecución de iediagcmd.exe y launch de comandos como route.exe desde directorios remotos.
4. Implementar Protecciones EDR / IPS con firmas específicas para detectar actividad relacionada con Horus Loader / Agent.
5. Educar al personal sobre riesgos de archivos .url recibidos por correo y advertir duplicación de extensiones o nombres engañosos.

**Prioridad: Crítica.**

**Ampliar Información:**

- <https://www.bleepingcomputer.com/news/security/stealth-falcon-hackers-exploited-windows-webdav-zero-day-to-drop-malware>
- <https://research.checkpoint.com/2025/stealth-falcon-zero-day/>
- <https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2025-patch-tuesday-fixes-exploited-zero-day-66-flaws/>

**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

### **Filefix: ataque que utiliza el explorador de Windows para ejecutar comandos Powershell de forma sigilosa**

Un nuevo vector malicioso llamado FileFix, detectado por el investigador *mr.d0x*, se aprovecha del Explorador de archivos de Windows para ejecutar comandos PowerShell sin interacción consciente del usuario. Es una evolución de los ataques ClickFix, ahora trasladados desde el navegador al entorno local de archivos.

Resumen técnico:

- El ataque induce al usuario a copiar una ruta especialmente diseñada, que incluye un fragmento PowerShell oculto mediante comentarios (; powershell ...), y luego pegarla en la barra de direcciones del Explorador de Windows.
- Esto ejecuta automáticamente el comando en un contexto local, con permisos del usuario, sin abrir el Símbolo del sistema ni PowerShell explícitamente.
- Al aprovechar un entorno confiable (Explorador de archivos), se reduce la sospecha para el usuario, facilitando la ejecución silenciosa de scripts maliciosos, descargas o cargas de malware.

Impacto potencial:

- Ejecución de scripts maliciosos sin permiso explícito.
- Descarga o instalación de malware (ransomware, info-stealers, RATs).

- Robo de credenciales, persistencia o movimiento lateral en la red.
- Reutilización como vector inicial en campañas más amplias.

#### Recomendaciones para mitigar el riesgo:

- Formación a usuarios sobre no ejecutar rutas copiadas de fuentes no confiables.
- Deshabilitar la PowerShell remota y restricciones de script mediante políticas de grupo (GPO).
- Configurar la AppLocker o Windows Defender Application Control para bloquear rutas no autorizadas o comandos desde el Explorador.
- Monitorear actividad relacionada con explorer.exe que invoque PowerShell con parámetros inusuales.
- Realizar auditoría continua de registros de PowerShell, identificando comandos pegados desde el Explorador.

#### **Prioridad: Urgente.**

#### **Ampliar Información:**

- <https://www.bleepingcomputer.com/news/security/filefix-attack-weaponizes-windows-file-explorer-for-stealthy-powershell-commands/>
- [https://www.linkedin.com/posts/avitechengineer\\_new-filefix-attack-weaponizes-windows-file-activity-7343310822401581057-IP-K](https://www.linkedin.com/posts/avitechengineer_new-filefix-attack-weaponizes-windows-file-activity-7343310822401581057-IP-K)
- <https://thehackernews.com/2025/06/new-filefix-method-emerges-as-threat.html>

