BOLETÍN CIBERSEGURIDAD

CSIRT - DATASEC

DataSec

# BoryptGrab roba datos en Windows mediante GitHub falso

**TLP:CLEAR**

16.03.2026

CLICK PARA EMPEZAR

CYBERSOCDTS

En esta edición: → El nuevo ladrón BoryptGrab ataca a los usuarios de Windows mediante páginas engañosas de GitHub

# CONTENIDO

DataSec

- Nuestra Esencia
- Vulnerabilidades
- Noticias
- Recomendaciones

# NUESTRA ESENCIA

## BOLETÍN CIBERSEGURIDAD

Este boletín está diseñado para mantener al lector informado y brindarle pautas de seguridad en un entorno digital en constante evolución. Incluye contenido sobre las últimas amenazas, vulnerabilidades y las mejores prácticas de protección.

## EMPRESA

DataSec es una empresa colombiana líder en servicios tecnológicos, enfocada en la implementación, administración, soporte, monitoreo y gestión de plataformas de Seguridad Informática y Networking, con años de experiencia en proyectos de ciberseguridad y conectividad para diversos sectores.

## SOC

DataSec cuenta con un Centro de Operaciones de Seguridad Cibernética (CSOC) especializado en la detección, análisis y respuesta a amenazas. Este centro opera de manera continua 24/7, contribuyendo a la prevención y mitigación de incidentes en tiempo real.

## Cisco Secure Firewall Management Center Software Authentication Bypass

**CVE-2026-20079**

**Critical (10.0)**

**Impacto:** Acceso y ejecución de comandos no autorizados

**Resumen:** Una vulnerabilidad de bypass de autenticación ("Authentication Bypass") [CWE-288] en la interfaz web de Cisco Secure Firewall Management Center (FMC), causada por la creación incorrecta de un proceso del sistema durante el arranque, podría permitir a un atacante remoto no autenticado omitir los mecanismos de autenticación y ejecutar archivos de script mediante solicitudes HTTP especialmente diseñadas.

### Producto Afectado

Producto compatible afectado:

- Cisco Secure Firewall Management Center (FMC) Software (múltiples versiones, incluyendo ramas 7.x y 10.x).

*Ver +INFO.*

### Solución:

Actualizar el software a las versiones corregidas publicadas por Cisco.

*Ver + INFO.*

Fecha de Publicación: 4/MAR/2026 INFO

## Unrestricted File Upload leading to Remote Code Execution

**CVE-2026-21536**

**Critical (9.8)**

**Impacto:** Ejecución remota de código

**Resumen:** Una vulnerabilidad de carga de archivos sin restricciones ("Unrestricted File Upload") [CWE-434] en Microsoft Devices Pricing Program, causada por una validación inadecuada del tipo y contenido de archivos cargados, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el servidor mediante la carga de archivos maliciosos especialmente diseñados.

### Producto Afectado

Producto compatible afectado:

- Microsoft Devices Pricing Program.

*Ver +INFO.*

### Solución:

Aplicar las actualizaciones de seguridad publicadas por Microsoft.

*Ver +INFO.*

Fecha de Publicación: 5/MAR/2026 INFO

## Authentication rate-limit bypass permits to brute force admin logins

**CVE-2026-24017**

**High (7.3)**

**Impacto:** Control de acceso inadecuado

**Resumen:** Una vulnerabilidad de control inadecuado de la frecuencia de interacción ("Improper Control of Interaction Frequency") [CWE-799] en Fortinet FortiWeb, causada por una implementación incorrecta del mecanismo de limitación de intentos de autenticación, podría permitir a un atacante remoto no autenticado evadir el límite de intentos de inicio de sesión mediante solicitudes especialmente diseñadas, aumentando la probabilidad de comprometer credenciales válidas.

### Producto Afectado

Producto compatible afectado:

- Fortinet FortiWeb versiones 8.0.0–8.0.2, 7.6.0–7.6.5, 7.4.0–7.4.10, 7.2.0–7.2.11 y 7.0.0–7.0.11.

*Ver +INFO.*

### Solución:

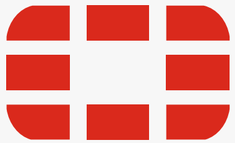
Actualizar Fortinet FortiWeb a las versiones corregidas publicadas por el proveedor cuando estén disponibles.

*Ver +INFO.*

Fecha de Publicación: 10/MAR/2026 INFO

## Stack-based Buffer Overflow in management service

**CVE-2025-54820**



**High (7.0)**

**Impacto:** Ejecución remota de código o comandos no autorizados

**Resumen:** Una vulnerabilidad de desbordamiento de búfer basado en pila ("Stack-based Buffer Overflow") [CWE-121] en Fortinet FortiManager, causada por el manejo inadecuado de datos de entrada en el servicio, podría permitir a un atacante remoto no autenticado ejecutar código o comandos no autorizados mediante solicitudes especialmente diseñadas. El éxito del ataque depende de la capacidad de evadir los mecanismos de protección de la pila.

### Producto Afectado

Producto compatible afectado:

- Fortinet FortiManager versiones 7.4.0 a 7.4.2, 7.2.0 a 7.2.10 y 6.4.

*Ver +INFO.*

### Solución:

Actualizar FortiManager a las versiones corregidas publicadas por el proveedor (por ejemplo 7.4.3, 7.2.11 o versiones posteriores).

*Ver +INFO.*

Fecha de Publicación: 10/MAR/206 INFO

## Mozilla Firefox Release

**CVE-2026-2757 – CVE-2026-2793**
**CVE-2026-2787 – CVE-2026-2774**

Mozilla ha publicado actualizaciones de seguridad para corregir múltiples vulnerabilidades en el navegador Firefox que incluyen errores de seguridad de memoria, fallas de validación de límites, entre otras. La explotación de estas podría permitir corrupción de memoria, ejecutar código arbitrario, causar denegación de servicio o evadir restricciones de seguridad mediante contenido web especialmente diseñado.

**Recomendación:**
Actualizar a la versión más reciente del navegador lo antes posible y aplicar las actualizaciones de seguridad correspondientes.

### Productos Afectados

Los productos afectados son:

- Mozilla Firefox versiones anteriores a 148
- Firefox ESR versiones anteriores a 115.33
- Firefox ESR versiones anteriores a 140.8

*Ver +INFO*

Fecha de Publicación: 24/FEB/2026 INFO

## Microsoft Release

**CVE-2026-21262 – CVE-2026-26127**
**CVE-2026-21415 – CVE-2026-21337**

Microsoft ha publicado actualizaciones para corregir múltiples vulnerabilidades en distintos componentes del ecosistema Windows. Estas fallas incluyen ejecución remota de código, elevación de privilegios, divulgación de información y denegación de servicio, las cuales podrían ser explotadas por atacantes para comprometer sistemas afectados.

**Recomendación:**
Aplicar las actualizaciones de seguridad liberadas por Microsoft lo antes posible.

### Productos Afectados:

Los productos afectados son:

- Microsoft Windows
- Windows Server y SQL Server
- Microsoft Edge (Chromium-based)
- Microsoft Office y otros componentes asociados

*Ver +INFO*

Fecha de Publicación: 10/MAR/2026 INFO

# LE PUEDE INTERESAR

| FECHA DE PUBLICACIÓN | CVE / ACCESO | FABRICANTE | CVSSV3 | DESCRIPCIÓN |
|---|---|---|---|---|
| 03/03/2026 | CVE-2026-20127 | Cisco | 10 | Permite que un atacante remoto sin credenciales válidas envíe solicitudes especialmente diseñadas para eludir el mecanismo de autenticación de peering, obteniendo así privilegios administrativos en el sistema afectado. Con ese acceso, el atacante puede interactuar con interfaces de gestión como NETCONF y modificar la configuración de la red SD-WAN con un usuario interno de alto privilegio. |
| 3/03/2026 | CVE-2026-1492 | WordPress | 9.8 | Permite que un atacante no autenticado cree cuentas con privilegios de administrador en el plugin de WordPress User Registration & Membership, tomando así control total del sitio afectado. |
| 4/03/2026 | CVE-2025-57740 | Fortinet | 6.7 | Permite que un usuario autenticado con privilegios bajos envíe peticiones especialmente diseñadas al componente de SSL-VPN RDP bookmark en dispositivos Fortinet, provocando un desbordamiento de búfer en memoria (heap) y llevando a que el atacante ejecute código no autorizado en el sistema afectado, comprometiendo potencialmente la confidencialidad, integridad y disponibilidad del dispositivo. |
| 11/03/2026 | CVE-2026-20116<br>CVE-2026-20117 | Cisco | 6.1 | Permite que un atacante autenticado con credenciales administrativas inyecte código malicioso en la interfaz web o ejecute comandos arbitrarios como root. |
| 4/03/2026 | CVE-2026-20006 | Cisco | 5.8 | Permite que un atacante remoto no autenticado envíe paquetes TLS especialmente diseñados a la Snort 3 Detection Engine de Cisco Secure Firewall Threat Defense (FTD) y provoque que el motor de detección se reinicie de forma inesperada, causando una condición de denegación de servicio (DoS) al dejar de inspeccionar y reenviar tráfico de red. |
| 26/02/2026 | CVE-2025-55018 | Fortinet | 5.2 | Permite que un atacante remoto no autenticado envíe peticiones HTTP especialmente diseñadas para aprovechar una falla de HTTP request smuggling en Fortinet FortiOS, logrando hacer pasar solicitudes que no quedan registradas por las políticas del firewall, lo que podría permitirle manipular el comportamiento del proxy/firewall y realizar acciones no autorizadas a través de cabeceras maliciosas. |

# BoryptGrab roba datos en Windows mediante repositorios falsos en GitHub

Investigadores de Trend Micro identificaron una campaña de malware llamada BoryptGrab, un information stealer dirigido principalmente a usuarios de Windows. Este malware está diseñado para robar información sensible como credenciales de navegadores, cookies, datos del sistema y archivos personales, además de información de billeteras de criptomonedas.
La campaña utiliza repositorios y páginas engañosas alojadas en GitHub para distribuir archivos maliciosos que aparentan ser software legítimo o herramientas gratuitas. En algunos casos, el malware también instala componentes adicionales que permiten a los atacantes mantener acceso remoto al equipo comprometido y continuar robando información.

A continuación, compartimos IoC para ser agregados a las herramientas de seguridad perimetral. Ver *+INFO*.

## El ATAQUE

El ataque se llevó a cabo mediante una campaña que utilizó repositorios falsos en GitHub para distribuir el malware. Los atacantes crearon más de 100 repositorios que aparentaban ofrecer software gratuito, herramientas de productividad, cheats de videojuegos o versiones crackeadas de programas populares.
Para atraer a las víctimas, los repositorios estaban optimizados con técnicas de SEO, lo que hacía que aparecieran en los primeros resultados de búsqueda cuando los usuarios buscaban descargar estos programas. Al entrar al repositorio y hacer clic en el enlace de descarga, los usuarios eran redirigidos a páginas falsas que generaban un archivo ZIP malicioso.
Dentro del archivo ZIP se incluían componentes que iniciaban la cadena de infección, como ejecutables que cargaban librerías maliciosas o scripts que descargaban el malware. Una vez ejecutado, el sistema quedaba infectado y BoryptGrab comenzaba a recolectar información sensible para enviarla a los atacantes.

INFO

| CONTEXT | INDICATOR | (MD5) |
|---|---|---|
| i0643k9.exe | fa767391b99865f8533efc1fe6dfa6175215718679fb00ca85fc13c3bd4ae4b7 | 8a9ac0c40f15bde54e5720e0dcbd7ab3 |
| WinUpdate | d295720bc0c1111ce1c3d8b1bc1b36ba840f103b3ca7e95a5a8bf03e2cc44fe5 | 8c291e8b260680e8c6d8adc683a44ff2 |
| scope-x-tool_2.5.6.vbs | 1bd605ef84b6767df74bd6290f1468eed5a88264df23fcf70b6a75d5bdcf7d76 | d8551563571e8f01c48a4c717810b7b9 |
| CryptoByte.exe | 4e90d386c1c7d3d1fd4176975795a2f432d95685690778e09313b4a1dbab9997 | e573630aa0a908265adff951a534a12a |
| vbs_app.exe | 4264a88035aa0b63e9aef96daa78a58114d60a344ea10168a8ef5ef36bf8edbd | 814b6e48edbd12e325ba87619c59f704 |
| EdgeUpdate | 7f2315b89fb9a47e1516def136844d617bfcdce19000a1b0436706692dbe166c | 48221bb8cb691be2daf4bcbea2da5b74 |
| launcher.exe | 449f528f5ceae8c3f8336d0d8e3e3ec9031d1ad67c31ee7311b67e01d5fdf225 | ffcc5ec07911e7d645bfdaf5767a885e |
| 91e8yoi.exe | c40b9913e79c5dd09751b1afb03aaa98658bab61bacf27a299abd84fd44fe707 | 9aa16d95fd7cc7af45f550db20790adf |
| WindowsRuntimeBroker.exe | 2abe0ef88ba92db79d82cde4c0ed1f382bb347517a54ea82084c841d0f955518 | 37e63c37d951649c131922e48ab52055 |
| client.exe | 576692df4bf1c7d8927d3a183f5219a81c3bff3dd22971691f8af6889f80c5a0 | b6d6e71bff9df5a99ba08258d2d53d31 |
| Dominio | http://193[.]143[.]1[.]104:5000/ | N/A |
| Dominio | http://45[.]93[.]20[.]195:5000/ | N/A |


INFO

# ÚLTIMAS NOTICIAS

## Malware en proyectos falsos de Next.js

Un grupo de atacantes lanzó una campaña dirigida a desarrolladores utilizando repositorios falsos de proyectos Next.js que se hacían pasar por pruebas técnicas o proyectos de entrevistas laborales. Cuando las víctimas descargaban y ejecutaban el código, se activaba JavaScript malicioso que se ejecutaba en memoria, permitiendo a los atacantes obtener acceso remoto al equipo, robar información sensible y establecer comunicación con servidores de comando y control (C2). El ataque aprovecha actividades normales de los desarrolladores, como clonar repositorios o ejecutar el servidor de desarrollo, para ocultar el malware dentro del flujo de trabajo habitual.

INFO

## VOID#GEIST multietapa distribuye RATs avanzados

La campaña de malware VOID#GEIST es un ataque multietapa que utiliza scripts ofuscados para distribuir diferentes troyanos de acceso remoto (RAT) como XWorm, AsyncRAT y Xeno RAT. El malware emplea archivos batch y un entorno de Python integrado para descifrar y ejecutar código malicioso directamente en memoria, lo que dificulta su detección por soluciones de seguridad. Además, el ataque utiliza técnicas avanzadas como inyección de código en el proceso explorer.exe mediante Early Bird APC injection, permitiendo a los atacantes mantener control del sistema comprometido y ejecutar múltiples cargas maliciosas sin dejar rastros evidentes en el disco.

INFO

## Nuevo bot de IA compromete repositorios de GitHub

Un bot impulsado por inteligencia artificial llamado Hackerbot-Claw llevó a cabo una campaña automatizada contra varios repositorios de GitHub relacionados con proyectos de empresas como Microsoft y DataDog. Este explotó configuraciones incorrectas en flujos de trabajo de CI/CD y GitHub Actions, lo que le permitió ejecutar código malicioso y robar credenciales o tokens con permisos de escritura en algunos proyectos. El ataque se realizó de forma rápida y automatizada, utilizando técnicas como inyección de nombres de archivos o ramas y manipulación de herramientas de desarrollo para infiltrarse en los repositorios.

INFO

# Ciberseguridad: más allá del teclado

Muchas veces pensamos que la ciberseguridad solo se trata de proteger nuestros datos en línea, pero la realidad es que la seguridad física también juega un papel fundamental. Un acceso físico no autorizado a servidores, centros de datos o equipos puede comprometer toda la infraestructura digital, sin importar cuán robustos sean nuestros sistemas.

🔐**Controla el acceso físico:** Usa candados, tarjetas de acceso y cámaras de seguridad en áreas sensibles como el datacenter.
🪪**Verifica la identidad**: Asegúrate de que solo personal autorizado pueda ingresar a zonas críticas.
💭**Capacita al equipo**: Promueve la conciencia sobre la importancia de cuidar tanto la información digital como los activos físicos.
👩‍🏫**Auditorías regulares**: Realiza inspecciones periódicas para detectar vulnerabilidades físicas.
📋**Políticas integrales**: Implementa normativas que abarquen tanto la seguridad digital como la física para proteger la organización en todos los frentes.

La seguridad completa protege tanto el mundo digital como el físico.

ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4