Incidente ID:	0015
Fecha del reporte:	06/11/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad Firewall de FortiWeb
Herramienta de detección	N/A
Activo involucrado:	Firewall de aplicaciones web FortiWeb
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la vulnerabilida de zero-day de Fortinet la cual se ha confirmado que está siendo explotada Activamente en el Firewall de Aplicaciones Web (WAF) FortiWeb de Fortinet.

Descripción:

Se ha identificado una vulnerabilidad crítica, explotada activamente como un posible ataque de día cero, en el Firewall de Aplicaciones Web (WAF) FortiWeb de Fortinet. La falla permite a un atacante remoto no autenticado crear una cuenta de administrador en los dispositivos vulnerables, obteniendo control total sobre el WAF y las aplicaciones que protege.

Se ha confirmado que la versión FortiWeb 8.0.1 (lanzada en agosto de 2025) es vulnerable. Fortinet ha lanzado la versión FortiWeb 8.0.2 para solucionar esta vulnerabilidad.

Se insta a todos los administradores a actualizar sus instancias de FortiWeb a la versión 8.0.2 de inmediato.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Productos afectados:

- Producto Afectado: Fortinet FortiWeb (Web Application Firewall)
- Versiones Vulnerables: FortiWeb 8.0.1 y anteriores.
- Versión Solucionada: FortiWeb 8.0.2
- Identificador CVE: Aún sin CVE asignado en el momento de este boletín, lo que subraya la naturaleza de día cero de la amenaza.
- Impacto: Creación de cuenta de administrador no autenticada (Control Total del Sistema).

Modo de explotación y cadena de infección

La vulnerabilidad está siendo explotada activamente en el mundo real. Un atacante puede enviar una solicitud HTTP especialmente diseñada a un dispositivo FortiWeb vulnerable.

Según los informes, la falla parece ser una vulnerabilidad de "path traversal" (salto de directorio) que permite a los atacantes invocar un script CGI interno no autorizado.

Se ha descubierto que el actor de amenazas detrás de la explotación envía una carga útil al punto final "/api/v2.0/cmdb/system/admin%3F/../../../../../cgi-bin/fwbcgi" mediante una solicitud HTTP POST para crear una cuenta de administrador.

Junto con la URI maliciosa, el atacante envía un cuerpo (body) en la solicitud POST. Este cuerpo es un objeto JSON que contiene los parámetros que el script fwbcgi espera recibir.

El script fwbcgi es un componente interno diseñado para gestionar usuarios, pero carece de su propia autenticación, asumiendo que cualquier cosa que lo llame ya ha sido autenticada.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Una explotación exitosa devuelve una respuesta HTTP 200 OK que contiene una respuesta JSON. Este JSON incluye detalles del nuevo usuario.

Algunos de los nombres de usuario y contraseñas de administrador creados por las cargas útiles detectadas en la naturaleza se muestran a continuación:

- Punto de prueba / AFodlUU3Sszp5
- comerciante1 / 3eMlXX43
- comerciante / 3eMlXX43
- test1234point / AFT3$tH4ck
- Punto de prueba / AFT3$tH4ck
- Punto de prueba / AFT3$tH4ckmet0d4yaga!n

Se informa que un supuesto exploit de día cero para esta falla se puso a la venta recientemente en un prominente foro de "sombrero negro" (black hat), lo que coincide con el inicio de la explotación activa.

Recomendaciones de mitigación:

Debido a la gravedad crítica y la explotación activa, se requieren acciones inmediatas.

1. Actualización Urgente

Actualice inmediatamente todas las instancias de FortiWeb a la versión 8.0.2 o superior. Esta versión ha sido confirmada como no vulnerable al exploit público.

En caso de presentar versiones antiguas del firewall y que no permite actualizar a la versión 8.0.2, a continuación se presenta las versiones en las cuales deben estar los firewalls web.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Versión	Afectado	Solución
FortiWeb 8.0	8.0.0 a 8.0.1	Actualiza a la versión 8.0.2 o superior.
FortiWeb 7.6	7.6.0 a 7.6.4	Actualiza a la versión 7.6.5 o superior.
FortiWeb 7.4	7.4.0 a 7.4.9	Actualiza a la versión 7.4.10 o superior.
FortiWeb 7.2	7.2.0 a 7.2.11	Actualiza a la versión 7.2.12 o superior.
FortiWeb 7.0	7.0.0 a 7.0.11	Actualiza a la versión 7.0.12 o superior.

2. Si la actualización inmediata no es posible, aplique la siguiente mitigación para reducir el riesgo:

- Restrinja el Acceso a la Interfaz de Gestión: La vulnerabilidad se explota a través de la interfaz de gestión del FortiWeb.
- Limite el acceso a esta interfaz para que solo sea accesible desde direcciones IP internas y de confianza (una "lista blanca").
- Nunca exponga la interfaz de gestión de FortiWeb directamente a Internet.

3. Se recomienda a todos los administradores, incluso después de parchear, que busquen señales de compromiso:

- Revise Cuentas de Administrador: Audite todas las cuentas de administrador en sus dispositivos FortiWeb. Busque cualquier cuenta desconocida o creada recientemente que no pueda ser verificada.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

– Revise los Logs del Servidor: Busque en los logs de acceso HTTP solicitudes POST sospechosas a la interfaz de gestión, especialmente aquellas que incluyan cgi-bin o patrones de "path traversal" (como .. / .. /)

Fuentes:

- https://www.rapid7.com/blog/post/etr-critical-vulnerability-in-fortinet-fortiweb-exploited-in-the-wild/
- https://www.techzine.eu/news/security/136346/fortiweb-vulnerability-actively-exploited-to-create-admin-accounts/
- https://www.techzine.eu/news/security/136346/fortiweb-vulnerability-actively-exploited-to-create-admin-accounts/
-

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570