I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de Incidente: Ejecución remota de código no autenticada y escalamiento de privilegios.

Nivel de riesgo: Alta

II. ALERTA

Figura 1. Vulnerabilidades en Fortinet de FortiWeb (CVE-2025-64446 - CVE-2025-58034) - figura referencial

FORTINET informó de dos vulnerabilidades catalogadas como críticas que afectan a su producto FortiWEB, CVE-2025-64446 es una vulnerabilidad de Relative Path Traversal que puede permitir la ejecución de comandos administrativos a través de crafted HTTP o HTTPS Request y CVE-2025-58034 es una vulnerabilidad de inyección de comandos del SO causada por la neutralización inadecuada de elementos controlados por el usuario tanto en los componentes API como CLI de FortiWeb.

III. INTRODUCCIÓN

CVE-2025-64446:

Es una vulnerabilidad de tipo Relative Path Traversal (CWE-23) que se origina por una validación insuficiente de las rutas de archivo proporcionadas por el usuario. Como

resultado, un atacante puede manipular dichas rutas para acceder a archivos y directorios ubicados fuera del directorio restringido establecido por la aplicación.

Como consecuencia, esta vulnerabilidad permite a un atacante remotamente ejecutar acciones con privilegios equiparables a los de un administrador, como la creación de nuevas cuentas de tipo administrador, establecer mecanismos de persistencia sin generar alertas y modificar parámetros de configuración, como los del firewall web.

CVE-2025-58034:

Es una vulnerabilidad clasificada como un error de Improper Neutralization of Special Elements in OS Command (CWE-78). Esta debilidad surge cuando una aplicación ejecuta comandos del sistema operativo basándose en datos proporcionados por el usuario sin aplicar una validación adecuada. Esto permite que un atacante inyecte elementos maliciosos en la entrada y provoque la ejecución de comandos no autorizados por parte del sistema operativo.

En este caso, la API y la CLI de FortiWeb validan incorrectamente los elementos especiales utilizados en los comandos del SO. Como resultado, un atacante autenticado puede ejecutar comandos arbitrarios en el sistema mediante el envío de solicitudes HTTP especialmente elaboradas o a través de entradas CLI manipuladas.

Los atacantes suelen encadenar vulnerabilidades para obtener acceso completo a los sistemas. En este caso, para explotar CVE-2025-58034, el atacante debe primero autenticarse en el dispositivo FortiWeb para la ejecución de comandos y es CVE-2025-64446 que permite a un atacante no autenticado obtener privilegios de administrador para la creación de usuarios, los cuales serán autenticados en el sistema.

IV. VECTOR DE ATAQUE

Esta vulnerabilidad en Fortinet de FortiWeb (CVE-2025-64446) posee una severidad CRITICAL con una puntación CVSS:3.1 de 9.8 tipo /AV:N /AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Esta vulnerabilidad en Fortinet de FortiWeb (CVE-2025-58034) posee una severidad ALTO con una puntación CVSS:3.1 de 7.2 tipo /AV:N /AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

V. IMPACTO

Los productos y versiones afectados son los siguientes:

Versión	Afectado
FortiWeb 8.0	Versión 8.0.0 a 8.0.1
FortiWeb 7.6	Versión 7.6.0 a 7.6.4
FortiWeb 7.4	Versión 7.4.0 a 7.4.9
FortiWeb 7.2	Versión 7.2.0 a 7.2.11
FortiWeb 7.0	Versión 7.0.0 a 7.0.11

Tabla 1.Versiones Afectadas - Vulnerabilidades en Fortinet de FortiWeb (CVE-2025-64446)

Versión	Afectado
FortiWeb 8.0	Versión 8.0.0 a 8.0.1
FortiWeb 7.6	Versión 7.6.0 a 7.6.5
FortiWeb 7.4	Versión 7.4.0 a 7.4.10
FortiWeb 7.2	Versión 7.2.0 a 7.2.11
FortiWeb 7.0	Versión 7.0.0 a 7.0.11

Tabla 2.Versiones Afectadas - Vulnerabilidades en Fortinet de FortiWeb (CVE-2025-58034)

VI. INDICADORES DE COMPROMISO

La vulnerabilidad CVE-2025-64446 tiene su blanco en:

- El módulo **fwcgi** de FORTIWEB, mediante un requerimiento HTTP POST en la Ruta **/api/v2.0/cmdb/system/admin%3F/../../../../../cgi-bin/**
- Otro indicador que se pudo apreciar es la creación de cuentas de usuarios de nombre: **Testpoint**, **trader** y **trader1**

Para la vulnerabilidad CVE-2025-58034

- Se centra en él envió de solicitudes HTTP manipuladas a la API de FortiWEB por medio CLI.

VII. RECOMENDACIONES:

- Se recomienda a las organizaciones que utilicen FortiWeb en versiones afectadas aplicar las actualizaciones a las siguientes versiones:

Versión	Solución
FortiWeb 8.0	Actualizar a 8.0.2 o superior
FortiWeb 7.6	Actualizar a 7.6.5 o superior
FortiWeb 7.4	Actualizar a 7.4.10 o superior
FortiWeb 7.2	Actualizar a 7.2.12 o superior
FortiWeb 7.0	Actualizar a 7.0.12 o superior

Tabla 3.Actualización de Versiones - Vulnerabilidades en Fortinet de FortiWeb (CVE-2025-64446)

Versión	Solución
FortiWeb 8.0	Actualizar a 8.0.2 o superior
FortiWeb 7.6	Actualice a 7.6.6 o superior
FortiWeb 7.4	Actualice a 7.4.11 o superior
FortiWeb 7.2	Actualizar a 7.2.12 o superior
FortiWeb 7.0	Actualizar a 7.0.12 o superior

Tabla 4. Actualización de Versiones - Vulnerabilidades en Fortinet de FortiWeb (CVE-2025-58034)

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

PICUS SECURITY (2025). FortiWeb CVE-2025-64446 Vulnerability: Path Traversal Leads to Remote Code Execution. https://www.picussecurity.com/resource/blog/fortiweb-cve-2025-64446-vulnerability-path-traversal-leads-to-remote-code-execution

ARCTIC WOLF (2025). CVE-2025-64446. https://arcticwolf.com/resources/blog/cve-2025-64446/

BITSIGHT (2025). Critical Vulnerability Alert: CVE-2025-64446 – Fortinet FortiWeb Vulnerability. https://www.bitsight.com/blog/critical-vulnerability-alert-cve-2025-64446-fortinet-fortiweb-vulnerability

WATCHTOWR LABS (2025). When the Impersonation Function Gets Used to Impersonate Users – Fortinet FortiWeb Auth Bypass**.** https://labs.watchtowr.com/when-the-impersonation-function-gets-used-to-impersonate-users-fortinet-fortiweb-auth-bypass/

CVE.ORG (2025). CVE-2025-64446. https://www.cve.org/CVERecord?id=CVE-2025-64446

CVE.ORG (2025). CVE-2025-58034. https://www.cve.org/CVERecord?id=CVE-2025-58034