La Agencia de Ciberseguridad y Seguridad de la Infraestructura de EE. UU. (CISA) incluyó el miércoles una vulnerabilidad crítica que afecta a los productos Fortinet en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), citando evidencia de que está siendo activamente explotada.

La vulnerabilidad, identificada como CVE-2024-23113 (con una puntuación CVSS de 9.8), está relacionada con la ejecución remota de código en FortiOS, FortiPAM, FortiProxy y FortiWeb.

> *«Una vulnerabilidad de cadena de formato controlada externamente [CWE-134] en el demonio fgfmd de FortiOS podría permitir que un atacante remoto y no autenticado ejecute código o comandos arbitrarios a través de solicitudes especialmente elaboradas»*, explicó Fortinet en un aviso sobre la falla publicado en febrero de 2024.

Como es común en estos boletines, hay poca información sobre cómo se está explotando esta vulnerabilidad en la práctica, o quién está utilizando esta falla y contra qué objetivos.

Debido a la explotación activa de esta vulnerabilidad, se exige a las agencias de la Rama Ejecutiva Civil Federal (FCEB) que apliquen las mitigaciones proporcionadas por el proveedor antes del 30 de octubre de 2024 para garantizar la máxima protección.

Palo Alto Networks revela fallos graves en Expedition

Palo Alto Networks también ha informado sobre varias vulnerabilidades críticas en su herramienta Expedition, que podrían permitir a los atacantes acceder a datos de bases de datos y archivos arbitrarios, además de escribir archivos en ubicaciones temporales del sistema.

> *«En conjunto, estos fallos exponen información como nombres de usuario, contraseñas en texto claro, configuraciones de dispositivos y claves API de los*

> *firewalls PAN-OS»*, señaló la compañía en una alerta el miércoles.

Version	Affected	Solution
FortiOS 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiOS 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiPAM 1.3	Not affected	Not Applicable
FortiPAM 1.2	1.2 all versions	Migrate to a fixed release
FortiPAM 1.1	1.1 all versions	Migrate to a fixed release
FortiPAM 1.0	1.0 all versions	Migrate to a fixed release
FortiProxy 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiProxy 7.2	7.2.0 through 7.2.8	Upgrade to 7.2.9 or above
FortiProxy 7.0	7.0.0 through 7.0.15	Upgrade to 7.0.16 or above
FortiWeb 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above

Las vulnerabilidades, que afectan a todas las versiones de Expedition anteriores a la 1.2.96, incluyen:

- CVE-2024-9463 (puntuación CVSS: 9.9): vulnerabilidad de inyección de comandos en el sistema operativo que permite a un atacante no autenticado ejecutar comandos arbitrarios como usuario root.
- CVE-2024-9464 (puntuación CVSS: 9.3): vulnerabilidad de inyección de comandos en el sistema operativo que permite a un atacante autenticado ejecutar comandos arbitrarios como root.

- CVE-2024-9465 (puntuación CVSS: 9.2): vulnerabilidad de inyección SQL que permite a un atacante no autenticado acceder al contenido de la base de datos de Expedition.
- CVE-2024-9466 (puntuación CVSS: 8.2): vulnerabilidad que expone información sensible en texto claro, lo que permite a un atacante autenticado ver nombres de usuario, contraseñas y claves API generadas.
- CVE-2024-9467 (puntuación CVSS: 7.0): vulnerabilidad de secuencias de comandos entre sitios (XSS) reflejada que permite la ejecución de JavaScript malicioso en el navegador de un usuario autenticado si este hace clic en un enlace malicioso, lo que podría llevar al robo de la sesión del navegador de Expedition.

La empresa reconoció a Zach Hanley de Horizon3.ai por descubrir y reportar las vulnerabilidades CVE-2024-9464, CVE-2024-9465 y CVE-2024-9466, y a Enrique Castillo de Palo Alto Networks por su trabajo en CVE-2024-9463, CVE-2024-9464, CVE-2024-9465 y CVE-2024-9467.

Aunque no se ha encontrado evidencia de que estas fallas hayan sido explotadas en el entorno real, se sabe que los métodos para reproducirlas ya están disponibles públicamente, según Horizon3.ai.

Existen alrededor de 23 servidores de Expedition expuestos en internet, la mayoría ubicados en EE. UU., Bélgica, Alemania, los Países Bajos y Australia. Como medida de mitigación, se recomienda limitar el acceso solo a usuarios, hosts o redes autorizadas y apagar el software cuando no esté en uso activo.

Cisco corrige un fallo en Nexus Dashboard Fabric Controller

La semana pasada, Cisco lanzó parches para corregir una vulnerabilidad crítica de ejecución de comandos en Nexus Dashboard Fabric Controller (NDFC), que surgió debido a una autorización inadecuada de usuarios y una validación insuficiente de los argumentos de comandos.

Esta vulnerabilidad, registrada como CVE-2024-20432 (con una puntuación CVSS de 9.9),

podría permitir que un atacante remoto autenticado, con pocos privilegios, realice un ataque de inyección de comandos en un dispositivo afectado. La falla ha sido corregida en la versión 12.2.2 de NDFC, mientras que las versiones 11.5 y anteriores no son vulnerables.

> *«Un atacante puede explotar esta vulnerabilidad enviando comandos diseñados a un punto de la API REST afectado o a través de la interfaz web. Si tiene éxito, el atacante podría ejecutar comandos arbitrarios en la CLI de un dispositivo gestionado por Cisco NDFC con privilegios de administrador de red»,* afirmó Cisco.