Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

DESCUBIERTA BACKDOOR EN VERSIONES EXPERIMENTALES DE FEDORA Y OTRAS DISTRIBUCIONES

30 / 03/ 2024

CONTENIDO

INTRODUCCIÓN

En un reciente descubrimiento que ha generado alarma en la comunidad de seguridad cibernética, se ha identificado una grave vulnerabilidad en las versiones experimentales de Fedora y otras distribuciones de Linux. La presencia de una puerta trasera en las bibliotecas de compresión de datos XZ Utils, especialmente en las versiones 5.6.0 y 5.6.1 de xz, ha puesto en riesgo la integridad y seguridad de los sistemas afectados. Este hallazgo, etiquetado como CVE-2024-3094, representa una amenaza crítica que requiere una acción inmediata por parte de los usuarios y desarrolladores para mitigar su impacto y proteger sus sistemas contra posibles ataques remotos.

DESCUBIERTA BACKDOOR EN VERSIONES EXPERIMENTALES DE FEDORA Y OTRAS DISTRIBUCIONES

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_03_30_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	30/03/2024
Es día cero (0 day):	No

RESUMEN

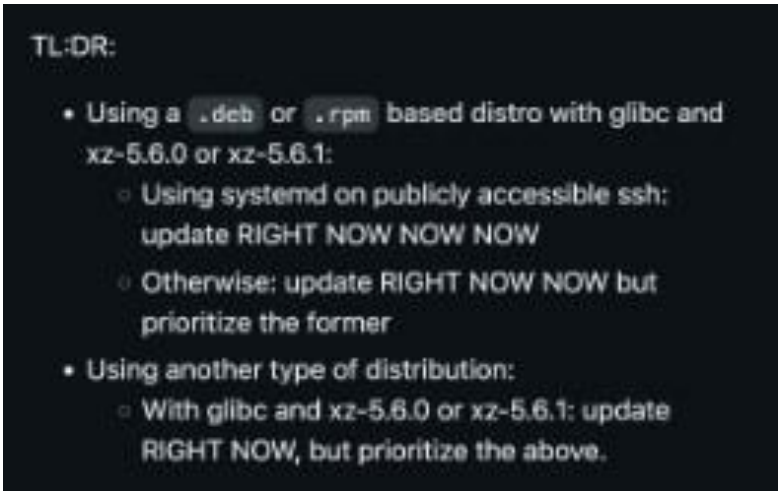
Recientemente, un alarmante hallazgo ha sacudido el mundo de la seguridad cibernética: se ha identificado una vulnerabilidad crítica en las versiones experimentales y de desarrollo de Fedora, así como en otras distribuciones de Linux. La preocupación radica en las bibliotecas de compresión de datos XZ Utils, específicamente en las versiones 5.6.0 y 5.6.1 de xz, donde se ha descubierto una puerta trasera maliciosa.

Detalles de la Vulnerabilidad

La vulnerabilidad, etiquetada como CVE-2024-3094, fue descubierta por el ingeniero de software de Microsoft, Andrés Freund, durante una investigación sobre anomalías en los inicios de sesión SSH en sistemas Linux. El código malicioso compromete la autenticación SSH a través de systemd, lo que abre la puerta a posibles ataques remotos por parte de actores malintencionados.

Impacto y Alcance de la Amenaza

El riesgo es significativo, ya que la vulnerabilidad afecta a varias distribuciones importantes, incluyendo Debian Sid, Fedora 41, Rawhide, Arch Linux 5.6.1x y NixoS unstable. La capacidad del código malicioso para interferir con la autenticación SSH representa una seria amenaza para la integridad y seguridad de los sistemas afectados.



Medidas de Mitigación y Respuesta Urgente

Ante esta amenaza inminente, se insta a los usuarios afectados a tomar medidas inmediatas para proteger sus sistemas. Se recomienda encarecidamente actualizar a versiones no comprometidas de XZ (5.4.6 Estable) o deshabilitar temporalmente SSH como medida de precaución. Además, se pueden utilizar herramientas como el script Bash creado por Andrés Freund y reglas de Yara para detectar y mitigar posibles actividades maliciosas.

Conclusiones y Acciones Futuras

Este descubrimiento subraya la importancia crítica de la vigilancia constante y las prácticas sólidas de seguridad cibernética en el entorno digital actual. La colaboración activa entre la comunidad de usuarios y desarrolladores es esencial para identificar, mitigar y prevenir activamente las amenazas cibernéticas. Solo mediante una respuesta coordinada y proactiva
podemos proteger eficazmente nuestros sistemas y datos contra los peligros del ciberespacio en constante evolución.

NOTICIA COMPLETA

https://devel.group/blog/descubierta-backdoor-en-versiones-experimentales-de-fedora-y-otras-distribuciones-que-debes-saber/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente