

ACTUALIZACIÓN CRÍTICA DE SEGURIDAD

Acción requerida para servidores Issabel.

Se ha identificado una vulnerabilidad crítica que está siendo explotada activamente contra servidores Issabel accesibles desde Internet.

La actualización oficial ya está disponible y debe instalarse inmediatamente.

ACTUALICE INMEDIATAMENTE

Instale todas las actualizaciones oficiales disponibles para Issabel.

Incluso si su servidor no presenta actividad sospechosa.

cloud.issabel.org/security-update-2026-08.php



POSIBLE IMPACTO

La actualización corrige la vulnerabilidad utilizada en esta campaña de ataques.



01 Control remoto del servidor.



02 Instalación persistente de malware (incluidos rootkits).



03 Compromiso de comunicaciones e información almacenada.

VERSIONES AFECTADAS

ISSABEL 4 `issabel-framework 4.0.0-12 o inferior`

ISSABEL 5 `issabel-framework 5.0.0-3 o inferior`





CÓMO ACTUALIZAR

Ejecute el comando correspondiente a su versión de Issabel.

ISSABEL 4

```
# yum --disablerepo=* --enablerepo=issabel-beta update  
issabel-framework
```

ISSABEL 5

```
# yum --disablerepo=* --enablerepo=issabel-cinco-beta  
update issabel-framework
```





DESPUÉS DE ACTUALIZAR

CÓMO VERIFICAR

Consulte la versión instalada del paquete:

```
# rpm -q issabel-framework
```

RESULTADO ESPERADO

ISSABEL 4 superior a 4.0.0-12

ISSABEL 5 superior a 5.0.0-3

Si continúa viendo una versión igual o inferior, repita la actualización o consulte el aviso oficial.



PREGUNTAS FRECUENTES

¿Debo actualizar si no veo actividad sospechosa?

SÍ La explotación es automatizada y puede no dejar señales visibles.

¿La actualización limpia un servidor ya comprometido?

NO Aísle el equipo de Internet y solicite una revisión de seguridad especializada.

¿Dónde descargo la actualización?

Únicamente desde los repositorios oficiales de Issabel.





GRACIAS POR AYUDAR A MANTENER SEGURA LA COMUNIDAD ISSABEL

Mantener los servidores actualizados fortalece la seguridad de toda la comunidad.

Consulte siempre el aviso oficial para obtener las instrucciones más recientes.

