BOLETÍN DE ALERTA

Boletín Nro.: 2022-10

Fecha de publicación: 22/02/2022

Fecha de actualización: 24/02/2022

Tema: Múltiples vulnerabilidades detectadas en *Zabbix Web Frontend*.

Software afectado:

- **Zabbix Frontend 6.0.0alpha1, 5.4.0 hasta 5.4.8.**
- **Zabbix Frontend 6.0.0 hasta 6.0.0beta1, 5.4.0 hasta 5.4.8.**

Descripción:

Se han detectado dos vulnerabilidades (CVE-2022-23131 y CVE-2022-23134) en *Zabbix Web Frontend*, que permitirían a un atacante evadir los sistemas de autenticación y obtener privilegios de administrador con el objetivo de poder realizar ejecución remota de código (RCE).

Estas vulnerabilidades se detallan a continuación:

- La vulnerabilidad identificada como CVE-2022-23131 de severidad critica, con una puntuación asignada de 9.8. Esta vulnerabilidad se debe a un error en la verificación de los datos de la sesión del usuario, lo cual permitiría a un atacante autenticado modificarlos logrando realizar escalamiento de privilegios, con el objetivo de realizar ejecución remota de código (RCE). Para realizar el ataque, se requiere que la autenticación SAML esté habilitada y el atacante debe conocer el nombre del usuario de Zabbix (o usar la cuenta de invitado, que está deshabilitada de forma predeterminada).

- La vulnerabilidad identificada como CVE-2022-23134 de severidad media, con una puntuación asignada de 5.3. Esta vulnerabilidad se debe a un error en los permisos de la configuración inicial del *Zabbix Web Frontend,* que permitiría el acceso de usuarios sin privilegios, a configuraciones críticas logrando así, evadir controles de seguridad y realizar cambios en la configuración del *Zabbix Web Frontend*.

Según los datos de Shodan Trends existen alrededor de 3800 instancias de *Zabbix Web Frontend* sin actualizar publicadas en Internet. CISA advierte sobre vulnerabilidades explotadas activamente en servidores Zabbix; existe una tendencia de explotación activa de estas vulnerabilidades, utilizando varias PoC (pruebas de conceptos) disponibles y publicadas en la red, con el fin de realizar ejecución remota de código (RCE), recomendamos la actualización de *Zabbix Web Frontend* los más pronto posible.

CISA ha agregado estas vulnerabilidades a su catálogo de vulnerabilidades conocidas y explotadas.

Impacto:

Un atacante podría obtener control total del sistema afectado a través de la ejecución remota de código (RCE).

Detección:

Para comprobar si su aplicación es vulnerable debe verificar si la versión de *Zabbix Web Frontend*, corresponde a las siguientes:

- CVE-2022-23131: *Zabbix Frontend* 6.0.0alpha1, 5.4.0 hasta 5.4.8.
- CVE-2022-23134: *Zabbix Frontend* 6.0.0 hasta 6.0.0beta1, 5.4.0 hasta 5.4.8.

Solución:

Se recomienda actualizar *Zabbix Web Frontend* a la última versión disponible 6.0, por medio de la siguiente guía:

- https://www.zabbix.com/documentation/current/en/manual/installation/upgrade

Si no es posible realizar una actualización inmediata, sugerimos deshabilitar la autenticación SAML, siguiendo la siguiente guía:

- https://www.zabbix.com/documentation/5.0/en/manual/web_interface/frontend_sections/administration/authentication#saml-authentication

Información adicional:

- https://www.zabbix.com/security_advisories
- https://support.zabbix.com/browse/ZBX-20350
- https://support.zabbix.com/browse/ZBX-20384
- https://blog.sonarsource.com/zabbix-case-study-of-unsafe-session-storage
- https://nvd.nist.gov/vuln/detail/CVE-2022-23134
- https://nvd.nist.gov/vuln/detail/CVE-2022-23131
- https://www.suse.com/security/cve/CVE-2022-23134.html
- https://thehackernews.com/2022/02/cisa-alerts-on-actively-exploited-flaws.html
- https://www.bleepingcomputer.com/news/security/cisa-warns-of-actively-exploited-vulnerabilities-in-zabbix-servers/