**CVE-2021-3156**

La vulnerabilidad CVE-2021-3156, también conocida como "Baron Samedit", fue una vulnerabilidad crítica de desbordamiento de búfer que afecta los sistemas operativos basados en Unix, incluidas varias distribuciones de Linux.

**Alias:** Baron Samedit

**Fecha de publicación:** 26 de enero de 2021

**Código CVE:** CVE-2021-3156

**Código CWE:** CWE-119 (Desbordamiento de búfer)

**Código CVSS explicado por partes:**

CVSS v3 Base Score: 7.2 (High)

Attack Vector (AV): Local (L)

Attack Complexity (AC): Low (L)

Privileges Required (PR): Low (L)

User Interaction (UI): None (N)

Scope (S): Unchanged (U)

Confidentiality (C): Low (L)

Integrity (I): High (H)

Availability (A): High (H)

**Boletín de seguridad**: La vulnerabilidad se incluyó en varios boletines de seguridad emitidos por diversas distribuciones de Linux, como Ubuntu, Red Hat, Debian, entre otras.

**Dirección de documentación:** Se pueden encontrar más información sobre la vulnerabilidad en el artículo oficial de Qualys, la empresa de seguridad que descubrió la vulnerabilidad: <https://blog.qualys.com/vulnerabilities-threat-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit>

**Software que afecta:** La vulnerabilidad afectó al programa sudo en versiones anteriores a la 1.9.5p2, utilizado ampliamente en sistemas Unix y Linux para otorgar a los usuarios privilegios de superusuario de forma controlada y segura.

**Descripción de la vulnerabilidad:** La vulnerabilidad permitía a un atacante local no autenticado ejecutar comandos con privilegios de superusuario utilizando una secuencia de comandos especialmente diseñada. Esto se debió a un desbordamiento de búfer en la función set\_cmnd del programa sudo.

**Repercusiones a nivel mundial y curiosidades:** La vulnerabilidad fue considerada crítica debido a su amplia distribución en sistemas Unix y Linux. Los atacantes podían explotarla para obtener acceso de superusuario a sistemas afectados, lo que les permitía realizar acciones maliciosas, como instalar malware, robar información confidencial o comprometer completamente el sistema. La naturaleza crítica de la vulnerabilidad y su explotación potencialmente dañina resaltaron la importancia de aplicar parches de seguridad de manera rápida y efectiva en los sistemas afectados.

**Importancia:** Esta vulnerabilidad fue importante debido a su gravedad y amplia distribución en sistemas Unix y Linux. Ilustró la necesidad crítica de mantener actualizados los sistemas y aplicar parches de seguridad de manera oportuna para protegerse contra amenazas cibernéticas significativas. La explotación exitosa de esta vulnerabilidad podría haber tenido consecuencias graves para la seguridad y la integridad de los sistemas afectados, lo que subraya la importancia de la vigilancia continua y la gestión proactiva de la seguridad de la información.