BOLETÍN DE ALERTA

Boletín Nro.: 2015-16
Fecha de publicación: 23/12/2015
Tema: Múltiples vulnerabilidades críticas en Joomla

Sistemas afectados:

- Joomla desde la versión 1.5 hasta la versión 3.4.6

Descripción:

En los últimos días se ha descubierto múltiples vulnerabilidades críticas que afectan a Joomla, en todas sus ramas. El equipo de Joomla ha publicado actualizaciones de seguridad para solucionar dichas vulnerabilidades.

La vulnerabilidad más crítica permite a atacantes remotos la ejecución de código arbitrario. Dicha vulnerabilidad está siendo explotado de forma activa en las últimas semanas, y ya se ha publicado exploits públicos que pueden ser utilizado por cualquier atacante para explotar dicha vulnerabilidad. Se le ha asignado el CVE-2015-8562 y afecta a las versiones de Joomla desde la 1.5 a las 3.4.5. Esta vulnerabilidad reside en el filtrado inadecuado de la información del "*user agent*" al guardar los valores de la sesión en la base de datos, lo que podría permitir la ejecución de código arbitrario. Para esta vulnerabilidad, debido a su gravedad, se han publicado actualizaciones incluso para las versiones 1.5.x y 2.5.x, fuera del ciclo de soporte.

Otra vulnerabilidad crítica de manejo de sesión igualmente podría permitir la ejecución remota de código, y afecta a todas las versiones de Joomla desde 1.5 a la 3.4.6. La causa de esta vulnerabilidad es un error en el propio PHP. Esto fue corregido por PHP en septiembre de 2015 con las versiones de PHP 4.5.45, 5.5.29, 5.6.13, por lo que los únicos sitios Joomla afectadas por este error son las que se encuentra alojado en versiones vulnerables de PHP. Sin embargo, teniendo en cuenta que no todos los servidores cuentan con una versión actualizada de PHP, Joomla publicó una actualización que corrige el error, para cualquiera de las versiones de PHP.

Además, se descubrió una vulnerabilidad de inyección de SQL, la cual también es corregida con la última actualización.

Para conocer más detalles acerca de cada una de estas vulnerabilidades, puede ver:

https://developer.joomla.org/security-centre/630-20151214-core-remote-code-execution-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

https://developer.joomla.org/security-centre/639-20151206-core-session-hardening.html

https://developer.joomla.org/security-centre/640-20151207-core-sql-injection.html

Impacto

Un atacante remoto no autorizado podría obtener un control total del servidor que aloja una aplicación web construida con una versión vulnerable de Joomla.

Solución

Joomla ha publicado una actualización, Joomla! 3.4.7 la cual corrige estas vulnerabilidades de seguridad críticas. 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 3.4.5. La nueva versión puede ser obtenida aquí:

https://www.joomla.org/announcements/release-news/5643-joomla-3-4-7-released.html

También se puede actualizar desde el panel de administración, siguiendo las recomendaciones oficiales:

https://www.joomla.org/announcements/release-news/5643-joomla-3-4-7-released.html

Para las versiones de Joomla fuera del ciclo de soporte (1.x y 2.x), si bien, se recuerda la importancia de migrar a una versión con soporte (3.x), se recomienda aplicar los parches de forma inmediata. Los mismos pueden ser obtenidos aquí:

https://docs.joomla.org/Security_hotfixes_for_Joomla_EOL_versions

Información adicional:

https://www.joomla.org/announcements/release-news/5643-joomla-3-4-7-released.html

https://www.joomla.org/announcements/release-news/5641-joomla-3-4-6-released.html

https://blog.sucuri.net/2015/12/remote-command-execution-vulnerability-in-joomla.html

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8562

https://docs.joomla.org/Security_hotfixes_for_Joomla_EOL_versions

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

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