computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2017-019

Joomla! Super User Password Leak

September 26, 2017 — v1.0

History:

- *26/09/2017 — v1.0 – Initial publication*

Summary

Joomla! is one of the most popular content management systems. According with the researches who reported this vulnerability, it powers about 3.3% of all websites' content [1].

A previously unknown LDAP injection vulnerability could allow remote attackers to leak the super user password with blind injection techniques and to fully take over any affected Joomla! installation. It is important to note, that in order to be vulnerable Joomla! has to be configured to use LDAP for authentication. Joomla! has fixed the vulnerability in the latest version 3.8.

The bug has received the number: CVE-2017-14596 by Mitre.

Products Affected

- Joomla! CMS versions 1.5.0 through 3.7.5

Recommendations

The bug has been fix in version 3.8.0, so it is recommended to update [2].

As workarounds – as far as the vulnerability affects the LDAP authentication, disabling it can be recommended for those who, for any reason, cannot update the CMS version (or in the meantime).

References

[1] https://blog.ripstech.com/2017/joomla-takeover-in-20-seconds-with-ldap-injection-cve-2017-14596/

[2] https://developer.joomla.org/security-centre/711-20170902-core-ldap-information-disclosure