CVE-2015-8562 – 16,000 Daily Attacks on vulnerable Joomla servers

December 28, 2015 By Pierluigi Paganini

Experts at Symantec discovered that hackers quickly take advantage of CVE-2015-8562 remote code execution to compromise Joomla servers.

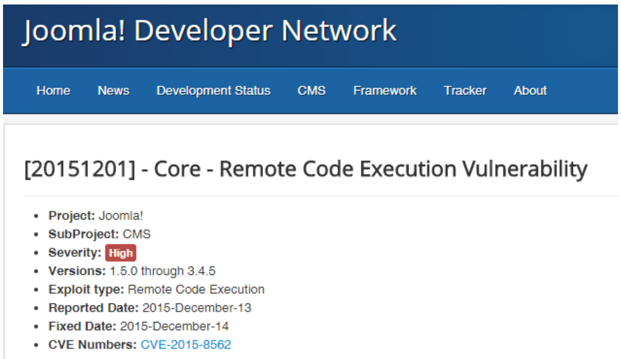
Joomla recently patched the CVE-2015-8562 vulnerability that could be exploited by attackers for remote code execution.

According to the security expert Daniel Cid from Sucuri, hundreds of attacks are now taking place.

"What is very concerning is that this vulnerability is already being exploited in the wild and has been for the last 2 days. Repeat: This has been in the wild as a 0-day for 2 days before there was a patch available." States *the blog post published by Sucuri.*

"The wave of attacks is even bigger, with basically every site and honeypot we have being attacked

The zero-day flaw could have a significant impact□ on the Internet users considering that Joomla is the most popular content management system having been downloaded more than 50 million times.



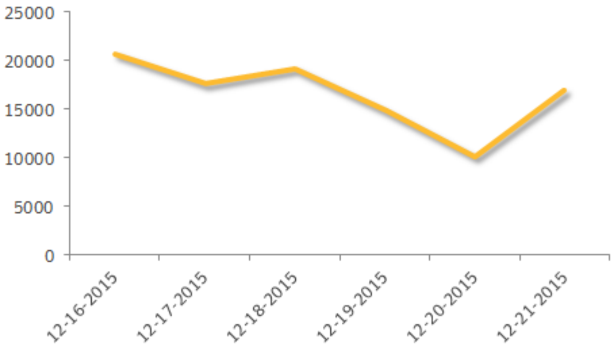
Joomla! Developer Network

[20151201] - Core - Remote Code Execution Vulnerability

- **Project:** Joomla!
- **SubProject:** CMS
- **Severity:** High
- **Versions:** 1.5.0 through 3.4.5
- **Exploit type:** Remote Code Execution
- **Reported Date:** 2015-December-13
- **Fixed Date:** 2015-December-14
- **CVE Numbers:** CVE-2015-8562

According to a security advisory published by Joomla, all versions above 1.5 are affected. It is important to update the CMS version to the patched version 3.4.6.

News of the day is that experts at Symantec have detected up to 20,000 daily attempts to exploit the Joomla CVE-2015-8562 vulnerability that has been fixed with the release of Joomla 3.4.6 and hotfixes□ for versions 1.5 and 2.5.

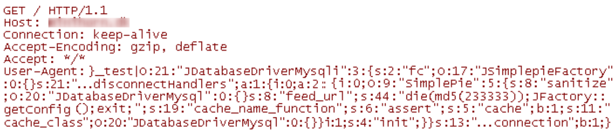


Symantec has been monitoring attack attempts against websites using vulnerable Joomla websites and detected, on average, 16,000 daily hits since the experts at Sucuri disclosed the flaw.□

"Since the Joomla! RCE vulnerability was discovered, servers running vulnerable versions of the CMS are actively being scanned for and attacked. On average, we are detecting more than 16,600 attacks per day on vulnerable Joomla! servers." states *Symantec.*

Cyber criminals exploit the CVE-2015-8562 vulnerability to fully compromise servers and abuse them to serve malware redirecting victims to exploit kits, or to launch other attacks such as distributed denial-of-service (DDoS) attacks.

"The exploit code is relatively easy to deploy and doesn't require much skill, all that is needed is a single HTTP request. According to our telemetry, the methods attackers are using to scan for vulnerable versions of Joomla! is similar to methods we covered in a recent blog on an RCE vulnerability in the vBulletin platform." states a blog post published by Symantec. "Attackers are scanning for servers running vulnerable versions of Joomla! by attempting to call a phpinfo*() function or printing out an MD5 of a predetermined value."*



```
GET / HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: }_test|O:21:"JDatabaseDriverMysqli":3:{s:2:"fc";O:17:"JSimplepieFactory"
:0:{}s:21:"...disconnectHandlers";a:1:{i:0;a:2:{i:0;O:9:"SimplePie":5:{s:8:"sanitize"
;O:20:"JDatabaseDriverMysql":0:{}s:8:"feed_url";s:44:"die(md5(233333));JFactory::
getConfig();exit;";s:19:"cache_name_function";s:6:"assert";s:5:"cache";b:1;s:11:"
cache_class";O:20:"JDatabaseDriverMysql":0:{}}i:1;s:4:"init";}}s:13:"...connection";b:1;}
```

According to researchers, threat actors in the wild are scanning the Internet searching for vulnerable servers, they are sending out HTTP requests and analyzing responses when functions such as*phpinfo()* and *eval(chr())* are executed.

Once the hackers identify a vulnerable server thay compromise it by installing a backdoor that allows them to control the machine and execute any kind of commands.

Administrators can check their web servers and examine access logs for suspicious activities, such as anomalous requests.

Pierluigi Paganini

(Security Affairs – CMS, CVE-2015-8562 vulnerability)

Share it please ...

Hacking Cybercrime zero-Day Joomla RCE CVE-2015-8562

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at□ Bit4Id, firm leader in identity□ management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field,□ he is Certified Ethical Hacker at□ EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog□ "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone,□ ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

Darkweb, a look back at 2015 events and 2016 predictions

NEXT ARTICLE

Database with 191 Million US voters' personal data exposed online

YOU MIGHT ALSO LIKE

Turkish hackers took over a Russian Govt Instagram account

January 3, 2016 By Pierluigi Paganini

Analyzing Ransom32, the first□ JavaScript ransomware variant

January 3, 2016 By Pierluigi Paganini

[redacted]

[redacted]

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for

Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top ^