Apache vulnerability is reported

21 September 2017, by Nancy Owano

Credit: Victorgrigas/Wikideia/ CC BY-SA 3.0

(Tech Xplore)—The Fuzzing Project blog this week carried a report we really do not like to hear but must know about regardless. Another "bleed" has been discovered. A bug in the Apache Web Server may result in contents from server memory being leaked.

Ars Technica and other sites have details but briefly this is where attackers could query servers and trick Apache into responding with more data.

The blog author is security researcher Hanno Böck who on September 18 said the leak involves something called the HTTP OPTIONS Method. What is OPTIONS? Böck explained that It is an HTTP method that allows asking a server which other HTTP methods it supports.

Ars Technica: The bug "causes servers to leak pieces of arbitrary memory in a way that could expose passwords or other secrets," Dan Goodin said.

Earlier on, when Böck had started searching for answers he contacted the Apache security team. "Fortunately Apache developer Jacob Champion digged into it and figured out what was going on." Apache supports a configuration directive, which he explained to Böck.

The root cause of the Optionsbleed was discovered, and patch files were made available for download.

What to do? His one word of advice if you run an Apache web server: Update. "Most distributions should have updated packages by now or very soon."

Böck provided patch links in his blog. Goodin also posted two links for patches.

However, Bock had more advice if you run an Apache web server in a shared hosting environment that allows users to create .htaccess files. Then, he said, "drop everything you are doing right now, update immediately and make sure you restart the server afterwards."

Paul Ducklin, *Naked Security*, described what goes wrong and why the name "Optionsbleed" makes sense. Ducklin wrote, "as far as Böck and Champion could tell, a memory mismanagement bug, provoked when Apache processes an .htaccess file that is meant to improve security…can end up reducing security by leaking data later on when a completely different part of Apache processes an OPTIONS request. Thus the name Optionsbleed."

So is this as bad as Heartbleed? Böck said it is not, as "this bug leaks only small chunks of memory and more importantly only affects a small number of hosts by default." But, he added, "It's still a pretty bad bug, particularly for shared hosting environments."

BleepingComputer's Security News Editor Catalin Cimpanu also explained how Heartbleed and Optionsbleed differ:

"Böck says Optionsbleed is not as severe as Heartbleed because it leaks content processed by

the Apache web server process only and not memory content from the underlying machine, including other applications. This means the leaked data is limited to whatever Apache is processing, which is mostly the content of web pages."

Cimpanu added: "Optionsbleed could leak content from pages that are only available to authenticated users."

Optionsbleed has a CVE, CVE-2017-9798.

Naked Security: "Whichever route you choose, keep your eye out for Apache's next official security update – the current patch may be replaced, improved, extended or superseded."

APA citation: Apache vulnerability is reported (2017, September 21) retrieved 2 July 2022 from https://techxplore.com/news/2017-09-apache-vulnerability.html