Patch Command Execution (CVE-2018-1000156)

Scott Court
April 6, 2018

What does it do?

This vulnerability allows for arbitrary code execution if the user goes to apply a malicious patch.

It does not require any special flags to be passed; it is the default behavior.

How was it found?

Patch for Holey Beep from https://holeybeep.ninja contained an exploit of this vulnerability.

This “patch” contained a line that would execute the “beep” command when the patch was applied.

How does it Work?

Uses the legacy ed patch format. This format allows for executing any valid ed command in a patch file.

Ed allows you to run a shell command, by prepending the shell command with a !

POC – Exploiting the Vulnerability

How to Fix It

A patch fixing this vulnerability was made available on 2018-04-06 at 12:23:02.

Now distribution maintainers need to apply this patch and push out an update...

Response from Distributions (As of 4/6/18 14:42 EDT)

Cucumber Linux – Fixed this morning

Debian – Waiting for patch

Arch Linux – Waiting for patch (severity: high)

SuSE – Pending (severity: moderate)

Ubuntu – Needs triage, no patch yet (severity: moderate)

Red Hat – Affected, work in progress for Red Hat 6 & 7

Will not fix on Red Hat 5

Severity: important

Interestingly Enough, FreeBSD and OpenBSD patched this same vulnerability in 2015.

POC – Patching the Vulnerability

Sidenote

<sidenote>

Cucumber Linux 1.1 was released this week. Go check it out at https://cucumberlinux.com/

</sidenote>

Questions?

Email: scott@cucumberlinux.com

This presentation can be found online at
https://cucumberlinux.com/~scott/presentations/

Further Reading:

https://security.cucumberlinux.com/security/details.php?id=355