Buffer overflow in command line unescaping

Todd C. Miller

Release Date:

January 26, 2021

Summary:

A serious heap-based buffer overflow has been discovered in sudo that is exploitable by any local user. It has been given the name *Baron Samedit* by its discoverer. The bug can be leveraged to elevate privileges to root, even if the user is not listed in the sudoers file. User authentication is not required to exploit the bug.

Sudo versions affected:

Sudo versions 1.8.2 through 1.8.31p2 and 1.9.0 through 1.9.5p1 are affected.

CVE ID:

This vulnerability has been assigned CVE-2021-3156 in the Common Vulnerabilities and Exposures database.

Details:

When sudo runs a command in *shell* mode, either via the **-s** or **-i** command line option, it escapes special characters in the command's arguments with a backslash. The sudoers policy plugin will then remove the escape characters from the arguments before evaluating the sudoers policy (which doesn't expect the escape characters) if the command is being run in shell mode.

A bug in the code that removes the escape characters will read beyond the last character of a string if it ends with an unescaped backslash character. Under normal circumstances, this bug would be harmless since sudo has escaped all the backslashes in the command's arguments. However, due to a different bug, this time in the command line parsing code, it is possible to run `sudoedit` with either the **-s** or **-i** options, setting a flag that indicates shell mode is enabled. Because a command is not actually being run, sudo does **not** escape special characters. Finally, the code that decides whether to remove the escape characters did not check whether a command is actually being run, just that the shell flag is set. This inconsistency is what makes the bug exploitable.

To test whether your version of sudo is vulnerable, the following command can be used:

```
sudoedit -s '\' `perl -e 'print "A" x 65536'`
```

If you receive a usage or error message, sudo is not vulnerable. If the result is a

Segmentation fault, sudo is vulnerable.

For more information, see The Qualys advisory.

Impact:

A local user may be able to exploit sudo to elevate privileges to root as long as the sudoers file (usually /etc/sudoers) is present.

Workaround:

None. Sudo version 1.9.5p2 or a patched vendor-supported version must be installed.

Fix:

The bug is fixed in sudo 1.9.5p2.

Credit:

Thanks to the Qualys Security Advisory team for their detailed bug report and explanation of its implications.