


Sudo爆可取得根帳號權限的漏洞

Sudo維護組織指出，從Sudo 1.7.1到1.8.25p1，都含有一項可讓用戶取得根帳號權限的漏洞，他們已在最新發布的1.8.31版完成修補，同時提供暫時緩解方法

文/ 林妍臻 | 2020-02-05 發表



About Sudo

- [Sudo Home](#)
- [A Short Introduction](#)
- [Stable Release](#)
- [Legacy Release](#)
- [Development Release](#)
- [A Brief History](#)
- [Contributors](#)
- [Sudo News](#)
- [NLS Support](#)
- [Sudo Plugins](#)
- [Sudo License](#)

Getting Sudo

- [Download Sudo](#) »
- [Browse Source](#)
- [Check out Source](#)
- [Mirroring Sudo](#)

Documentation

Sudo Stable Release

Current Stable Release

The current stable release of **sudo** is **1.8.31**.

For full details see the [ChangeLog](#) file or view the commit history via [mercurial](#).

Major changes between version 1.8.31 and 1.8.30:

- Fixed **CVE-2019-18634**, a buffer overflow when the *pwfeedback* sudoers option is enabled on systems with uni-directional p
- The *sudoedit_checkdir* option now treats a user-owned directory as writable, even if it does not have the write bit set at the l links will no longer be followed by sudoedit in any user-owned directory. [Bug #912](#).
- Fixed sudoedit on macOS 10.15 and above where the root file system is mounted read-only. [Bug #913](#).
- Fixed a crash introduced in sudo 1.8.30 when suspending sudo at the password prompt. [Bug #914](#).
- Fixed compilation on systems where the mmap MAP_ANON flag is not available. [Bug #915](#).

Major changes between version 1.8.30 and 1.8.29:

- Fixed a warning on macOS introduced in sudo 1.8.29 when sudo attempts to set the open file limit to unlimited. [Bug #904](#).
- Sudo now closes file descriptors before changing uids. This prevents a non-root process from interfering with sudo's ability t on systems that support the prlimit(2) system call.
- Sudo now treats an attempt to run `sudo sudoedit` as simply `sudoedit` If the sudoers file contains a fully-qualified path to sudo

Sudo維護組織已在最新1.8.31版，修補了CVE-2019-18634漏洞，該漏洞可讓用戶觸發緩衝溢位，取得根帳號權限。



Linux/Unix平台知名管理工具Sudo爆發漏洞，可讓用戶觸發緩衝溢位，取得根帳號權限。所幸Sudo維護組織已經修補該漏洞並釋出最新版本。

Sudo是Unix/Linux平台管理廣受歡迎的工具，它讓系統管理員可分配給一般用戶合理的權限，以執行一些只有管理員或其他特定帳號才能完成的任務。

最新編號CVE-2019-18634的漏洞，出在一個pwfeedback的功能選項中。這個功能讓系統可以星號字元表示目前輸入的字元長度，原本是提升安全性的功能，但蘋果資訊安全研究員Joe Vennix發現，sudoer檔案開啟pwfeedback功能後，可能讓用戶觸發堆疊式（stack-based）緩衝溢位攻擊，讓沒有系統管理權限的用戶、甚至連非列於sudoer檔案中的用戶得以提升到根帳號。由於攻擊者完全掌控資料控制權以發動緩衝溢位，因此本漏洞被開採機率極高。

Sudo維護組織指出，Sudo 1.7.1到1.8.25p1都受本漏洞影響，不過前提是系統管理員需開啟pwfeedback，未開啟者就不需要擔心。另外，1.8.26到1.8.30版也出現CVE-2019-18634，但1.8.26版本時曾變更EOF（end of file）處理的設定，致使該漏洞無法被開採。

Pwfeedback在sudo上游版本中預設關閉，但在Linux Mint及Elementary OS中卻是預設開啟的。所幸Sudo組織已經釋出最新版1.8.31版，應該也會很快部署到所有主要Linux發行版或macOS中。

如果尚未能安裝更新版本，在開啟pwfeedback的sudoer檔內，將「Defaults pwfeedback」改成「Defaults !pwfeedback」，也能有效阻止攻擊。








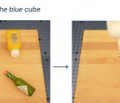


iThome Security

追蹤粉絲專頁2萬位追蹤者



熱門新聞

	美澳政府警告影響微軟Teams的IDOR竊密漏洞可能被大量濫用 2023-07-31		歐盟將調查微軟Office、Teams網綁行為 2023-07-31
	【資安日報】7月28日，惡意軟體Nitrogen被用於勒索軟體攻擊，並透過Google、Bing廣告散布 2023-07-28		【資安週報】2023年7月24日到7月28日 2023-07-31
	研究人員警告，4成Ubuntu含有漏洞風險 2023-07-28		去年發現41個遭到攻擊的零時差漏洞，Android上的n-days漏洞跟0-days漏洞一樣危險 2023-07-31
	Stability AI公布最新文字轉圖片模型Stable Diffusion XL 1.0 2023-07-28		Google發表首個可同時理解文字與視覺，並完成任務的Robotic Transformer 2 2023-07-31

