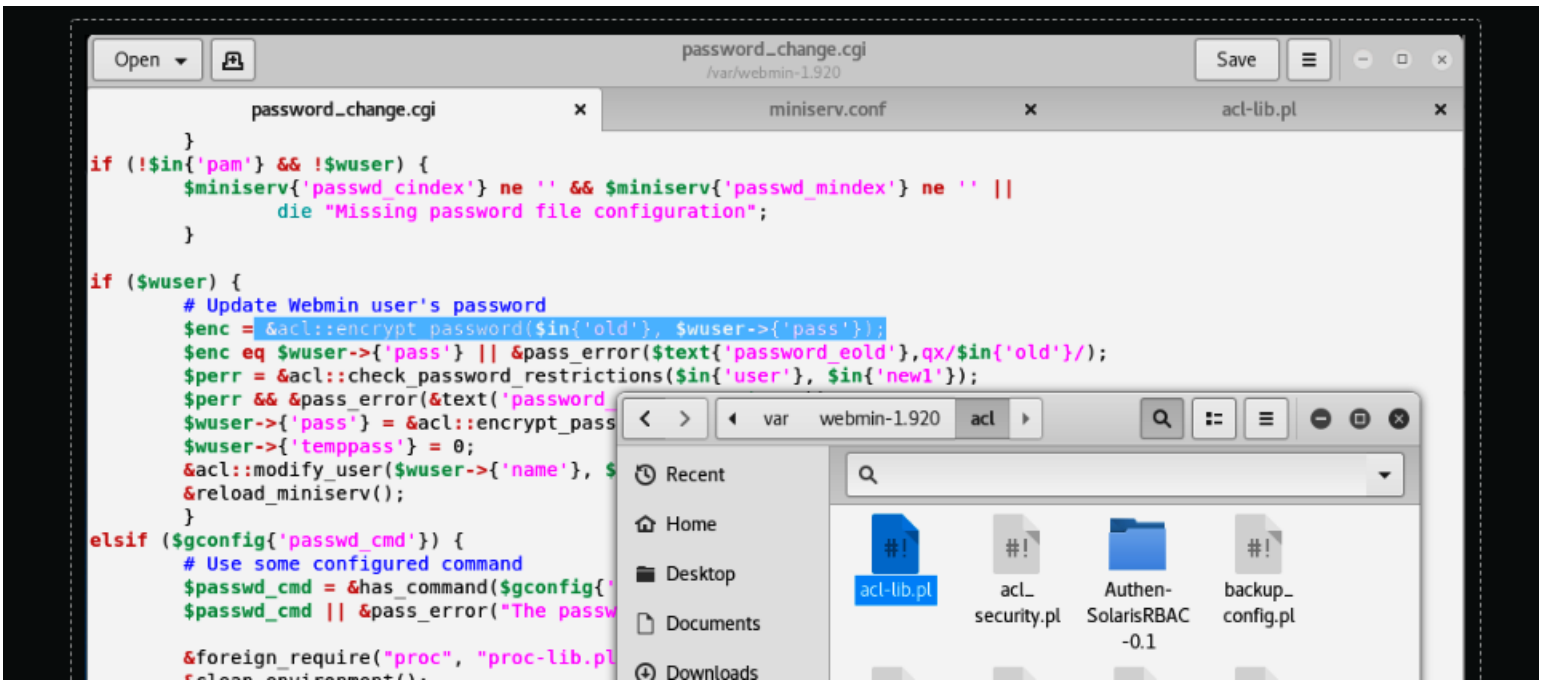
新聞

Unix管理工具Webmin爆有遠端程式碼執行漏洞

漏洞存在於Webmin在1.920之前的版本，可讓遠端駭客以根權限執行惡意指令

文/ 林妍溱 | 2019-08-20 發表



土耳其安全研究人員Özkan Mustafa Akkuş發現Webmin上出現遠端程式碼執行漏洞，影響1.920版本以前的Webmin，它出在password_change.cgi元件中一段程式碼中。許多webmin管理員都會開啟「user password change」的功能，它讓使用者可以將過期舊密碼重設為新密碼。研究人員發現，只要在傳送的指令參數中包含old引數（Argument），password_change.cgi看到有old就驗證通過，不論輸入的用戶名稱、舊密碼或其他資訊是否正確。（圖片來源／Özkan Mustafa Akkuş）

廣受歡迎的Unix類伺服器Web化管理工具Webmin被發現有遠端程式碼執行（RCE）漏洞，可讓遠端駭客以根權限執行惡意指令。

Webmin是許多Unix作業系統如Linux、FreeBSD、OpenBSD等遠端系統管理員愛用的Web app，可用以修改OS設定、建立用戶帳號、管理磁碟容量、檔案或服務，以及管理遠端伺服器上的軟體如Apache HTTP Server、BIND DNS Server、MySQL、PHP、Exim等等。Webmin官方GitHub網頁宣稱其全球用戶超過百萬。

土耳其安全研究人員Özkan Mustafa Akkuş近日發現Webmin上出現遠端程式碼執行（remote code execution，RCE）漏洞，並在上周的AppSec Village大會上公佈。

這個編號CVE-2019-15107的漏洞影響1.920版本以前的Webmin，它出在password_change.cgi元件中一段程式碼中。許多webmin管理員都會開啟「user password change」的功能，它讓使用者可以將過期舊密碼重設為新密碼。

研究人員發現，只要在傳送的指令參數中包含old引數（Argument），password_change.cgi看到有old就驗證通過，不論輸入的用戶名稱、舊密碼或其他資訊是否正確，這即可達成權限升級，允許未獲授權攻擊者在Webmin app輸入任何指令，進而控制執行Webmin的Unix、Linux伺服器。CVE-2019-15107被列為重大（critical）風險。

Webmin維護團隊周一指出，這並不是程式編寫的瑕疵，而是「程式撰寫基礎架構有漏洞遭惡意程式碼注入」的結果。維護團隊也在周一修補漏洞並發佈新（1.930）版本Webmin及Usermin，可從SourceForge下載。

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綑綁行為

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

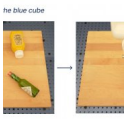
2023-07-28

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

電週文化事業版權所有、轉載必究 | Copyright © iThome 刊登廣告 訂閱週刊 授權服務 服務信箱
隱私權聲明與會員使用條款 關於iThome RSS 徵才