Vulnerabilities in Thunderbird Email Client Allow Code Execution

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/aNzl4k6txE0/vulnerabilities-thunderbird-email-client-allow-code-execution

---

Yubico Replacing YubiKey FIPS Devices Due to Security Issue

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/GQFxrrydlZg/yubico-replacing-yubikey-fips-devices-due-security-issue

---

Critical Vulnerabilities Found in WAGO Industrial Switches

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/eVcAeJp7k00/critical-vulnerabilities-found-wago-industrial-switches

XSS Vulnerability Exposed Google Employees to Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/dBzsdKuLGYs/xss-vulnerability-exposed-google-employees-attacks

---

If you haven’t patched Vim or NeoVim text editors, you really, really should

reader comments

134 with 81 posters participating

Share this story

A recently patched vulnerability in text editors preinstalled in a variety of Linux distributions allows hackers to take control of computers when users open a malicious text file. The latest version of Apple’s macOS is continuing to use a vulnerable version, although attacks only work when users have changed a default setting that enables a feature called modelines.

Vim and its forked derivative, NeoVim, contained a flaw that resided in modelines. This feature lets users specify window dimensions and other custom options near the start or end of a text file. While modelines restricts the commands available and runs them inside a sandbox that’s cordoned off from the operating system, researcher Armin Razmjou noticed the source command (including the bang on the end) bypassed that protection.

“It reads and executes commands from a given file as if typed manually, running them after the sandbox has been left,” the researcher wrote in a post earlier this month.

The post includes two proof-of-concept text files that graphically demonstrate the threat. One of them opens a reverse shell on the computer running Vim or NeoVim. From there, attackers could pipe commands of their choosing onto the commandeered machine.

“This PoC outlines a real-life attack approach in which a reverse shell is launched once the user opens the file,” Razmjou wrote. “To conceal the attack, the file will be immediately rewritten when opened. Also, the PoC uses terminal escape sequences to hide the modeline when the content is printed with cat. (cat -v reveals the actual content.)”

The researcher included the following GIF image:

The command-execution vulnerability requires that the standard modelines feature be enabled, as it is in some Linux distributions by default. The flaw resides in Vim prior to version 8.1.1365 and in Neovim before version 0.3.6. This advisory from the National Institute of Standards and Technology's National Vulnerabilities Database shows that both the Debian and Fedora distributions of Linux have begun issuing patched versions. Linux users should make sure the update gets installed, particularly if they're in the habit of using one of the affected text editors.

Interestingly, Apple's macOS, which has long shipped with Vim, continues to offer a vulnerable version 8 of the text editor. Modelines isn't enabled by default, but in the event a user turns it on, at least one of the Razmjou PoCs work, Ars has confirmed. Apple representatives didn't respond to an email seeking comment for this post.

https://arstechnica.com/?p=1521597

Microsoft Patches Critical Vulnerabilities in NTLM

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Mh06XbZCxL4/microsoft-patches-critical-vulnerabilities-ntlm

---

New RAMBleed Attack Allows Access to Sensitive Data in Memory

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/TnBdmic9i_s/new-rambleed-attack-allows-access-sensitive-data-memory

---

Adobe Patches Code Execution Flaws in Flash, ColdFusion, Campaign

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/B3wS1C-EkEs/adobe-patches-code-execution-flaws-flash-coldfusion-campaign

---

Critical Oracle WebLogic Vulnerability Exploited in Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/EU8ruAJ

sJms/critical-oracle-weblogic-vulnerability-exploited-attacks

---

VMware Patches Vulnerabilities in Tools, Workstation

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/xg9akm5ySeg/vmware-patches-vulnerabilities-tools-workstation