

Notepad++ users take note: It's time to check if you're hacked

According to independent researcher Kevin Beaumont, three organizations told him that devices inside their networks that had Notepad++ installed experienced “security incidents” that “resulted in hands on keyboard threat actors,” meaning the hackers were able to take direct control using a web-based interface. All three of the organizations, Beaumont said, have interests in East Asia.

The researcher explained that his suspicions were aroused when Notepad++ version 8.8.8 introduced bug fixes in mid-November to “harden the Notepad++ Updater from being hijacked to deliver something... not Notepad++.”

The update made changes to a bespoke Notepad++ updater known as GUP, or alternatively, WinGUP. The gup.exe executable responsible reports the version in use to <https://notepad-plus-plus.org/update/getDownloadUrl.php> and then retrieves a URL for the update from a file named gup.xml. The file specified in the URL is downloaded to the %TEMP% directory of the device and then executed.

Beaumont wrote:

If you can intercept and change this traffic, you can redirect the download to any location it appears by changing the URL in the property.

This traffic is supposed to be over HTTPS, however it appears you may be [able] to tamper with the traffic if you sit on

the ISP level and TLS intercept. In earlier versions of Notepad++, the traffic was just over HTTP.

The downloads themselves are signed—however some earlier versions of Notepad++ used a self signed root cert, which is on Github. With 8.8.7, the prior release, this was reverted to GlobalSign. Effectively, there's a situation where the download isn't robustly checked for tampering.

Because traffic to notepad-plus-plus.org is fairly rare, it may be possible to sit inside the ISP chain and redirect to a different download. To do this at any kind of scale requires a lot of resources.

Beaumont published his working theory in December, two months to the day prior to Monday's advisory by Notepad++. Combined with the details from Notepad++, it's now clear that the hypothesis was spot on.

<https://arstechnica.com/security/2026/02/notepad-updater-was-compromised-for-6-months-in-supply-chain-attack/>