NVIDIA Patches Serious Flaw in GeForce Experience Software

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/D7NVI7VSh2M/nvidia-patches-serious-flaw-geforce-experience-software

---

Apple Patches Vulnerabilities in iOS, macOS, Safari

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/q3bthb45ays/apple-patches-vulnerabilities-ios-macos-safari

---

New Settings Help Hackers Test Facebook Mobile Apps

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/jX9T7leKFF0/new-settings-help-hackers-test-facebook-mobile-apps

Microsoft Finds Privilege Escalation, Code Execution Flaws in Huawei Tool

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/CDy0OzSpEQ0/microsoft-finds-privilege-escalation-code-execution-flaws-huawei-tool

---

Major U.S. Chemical Firms Hit by Cyberattack

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/4nX-qTjx0nY/major-us-chemical-firms-hit-cyberattack

---

Second Critical Crypto Flaw Found in Swiss E-Voting

System

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/bezZ_CP1xG8/second-critical-crypto-flaw-found-swiss-e-voting-system

---

Cisco Patches High Severity Vulnerabilities in IP Phones

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/yrGDjec2NDs/cisco-patches-high-severity-vulnerabilities-ip-phones

---

Pwn2Own 2019: Researchers Win Tesla After Hacking Its Browser

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/zJYBipjrItY/pwn2own-2019-researchers-win-tesla-after-hacking-its-browser

---

Two serious WordPress plugin vulnerabilities are being exploited in the wild



reader comments

30 with 20 posters participating

Share this story

Attackers have been actively exploiting serious vulnerabilities in two widely used WordPress plugins to compromise websites that run the extensions on top of the content management system.

The two affected plugins are Easy WP SMTP with 300,000 active installations and Social Warfare, which has about 70,000 active installations. While developers have released patches

for both exploited flaws, download figures indicate many vulnerable websites have yet to install the fixes. Figures for Easy WP SMTP, which was fixed five days ago, show the plugin has just short of 135,000 downloads in the past seven days. Figures for Social Warfare show it has been downloaded fewer than 20,000 times since a patch was published on WordPress on Friday. Sites that use either plugin should disable them immediately and then ensure they have been updated to version 1.3.9.1 of Easy WP SMTP and 3.5.3 of Social Warfare.

Attacks exploiting Easy WP SMTP were first reported by security firm NinTechNet on Sunday, the same day a patch became available. On Wednesday, a different security firm, Defiant, also reported the vulnerability was under active exploit despite the availability of the patch. The exploits allow attackers to create rogue administrative accounts on vulnerable websites.

Two competing groups appear to be carrying out the attacks, Defiant reported. One group stops after creating the administrative accounts. The other group uses the rogue accounts to make site changes that redirect visitors to malicious sites. Interestingly, both groups create the accounts using the same attack code, which was initially published as a proof-of-concept exploit by NinTechNet. The latter group uses two domains—setforconfigplease[.]com, and getmyfreetraffic[.]com—to track redirected users. As of Thursday, researchers with security firm Sucuri said they also continued to detect exploits in the wild.

Attacks against Social Warfare, meanwhile, are permitting serious hacks against vulnerable sites. According to Defiant, attackers are exploiting a flaw that allowed anyone visiting a vulnerable site to overwrite its plugin settings. The attackers use that ability to make the site vulnerable to a cross-site scripting attack that pulls malicious payloads off Pastebin pages and execute them in visitors’ browsers.

The payloads redirect visitors to malicious sites. At the time this post was going live, two of the malicious Pastebin pages—https://pastebin.com/raw/0yJzqbYf and https://pastebin.com/raw/PcfntxEs—had yet to be taken down. One of the two domains contained in the payloads is setforconfigplease[.]com, which is being used in some of the exploits against Easy WP SMTP.

“These domains are part of a larger redirect campaign, and are both hosted on the same IP address, 176.123.9.52,” Defiant researcher Mikey Veenstra wrote. “Visitors who are redirected to these addresses are subsequently redirected to a series of malicious sites, and their individual activity is tracked via cookies. Reports have indicated a variety of eventual redirect targets, from pornography to tech support scams.”

As noted earlier, sites that use either of these WordPress plugins are at immediate risk of being compromised and should update at once. In the event updating isn’t immediately possible—for instance, if updates cause crashes as some users of Social Warfare claim—website developers should disable the plugin until an update is successful.

The attacks are a good reminder to end users that they can be redirected to malicious sites even when visiting trusted sites that have had good track records with security in the past. Web users should remember, too, that malicious sites are often designed to look identical to operating system warnings that there is a serious problem. The best thing someone can do when redirected to a malicious site is to attempt to force quit the browser or browser tab. If that doesn’t work, consider leaving the page alone and seeking help from someone else. Under no circumstances should people call displayed numbers or download or install software linked in one of these redirects despite urgently worded advisements to the contrary.

https://arstechnica.com/?p=1479063

Researchers Earn $270,000 for Firefox, Edge Hacks at Pwn2Own 2019

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/qgxxi2j5bWY/researchers-earn-270000-firefox-edge-hacks-pwn2own-2019