ACROS Security Launches 0patch PRO

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/UZ3B3blAci0/acros-security-launches-0patch-pro

---

PoC Exploits Released for Unpatched Edge, IE Vulnerabilities

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/y_KayAwMRHk/poc-exploits-released-unpatched-edge-ie-vulnerabilities

---

JavaScript Library Introduced XSS Flaw in Google Search

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/61aVmtvkMSs/javascript-library-introduced-xss-flaw-google-search

Magento Patches Critical Vulnerabilities

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Ax6umQDJkic/magento-patches-critical-vulnerabilities

---

Serious Path Traversal Flaw Found in Kubernetes

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Hf7PfbSnEM0/serious-path-traversal-flaw-found-kubernetes

---

Brace yourselves: exploit published for serious Magento bug allowing card skimming (Updated)



reader comments

57 with 48 posters participating

Share this story

Attack code was published on Friday that exploits a critical vulnerability in Magento e-commerce platform, all bug guaranteeing it will be used to plant payment card skimmers on sites that have yet to install a recently released patch.

PRODSECBUG-2198 is a SQL injection vulnerability that attackers can exploit with no authentication required. Hackers could exploit the flaw to take administrative control of administrator accounts, assuming the hackers can download user names and password hashes and crack the hashes. From there, attackers could install the backdoors or skimming code of their choice. A researcher at Web security firm Sucuri said Thursday that company researchers reverse-engineered an official patch released Tuesday and successfully created a working proof of concept exploit.

Over the past six months, a raft of competing crime gangs has been racing to infect commerce sites with JavaScript that surreptitiously steals purchasers' credit card data. The compromises are the result of exploits against either known or zeroday vulnerabilities. A vulnerability of this severity in an e-commerce platform that boasts 300,000 businesses and merchants is almost certainly going to face in-the-wild attacks by the same card-skimmer gangs.

"There is no doubt threat actors are either actively reversing the patch or waiting for a proof of concept to exploit this flaw at scale," Jérôme Segura, lead malware intelligence analyst at Malwarebytes, told Ars on Thursday. "When it comes to hacked Magento websites, Web skimmers are the most common infection type we see because of their high return on investment. As a result, we can expect another wave of compromises in light of this newly found critical vulnerability."

On Friday, a proof-of-concept exploit were published here. Comments in the code say it "can easily be modified to obtain other stuff from the [database], for instance admin/user password hashes." It also says the underlying vulnerability has resided in Magento since version 1. That means virtually all Magento sites that haven't installed the patch are susceptible. A separate technical writeup here, also published Friday, provides additional exploit details, along with the disclosure timeline.

"As predicted, we are going to see sites getting hacked pretty soon," Segura wrote in an email Friday, after learning of the new posts.

Sucuri researcher Marc-Alexandre Montpas concurred with that assessment. In Thursday's blog post, he wrote:

> *SQL Injections allow an attacker to manipulate site arguments to inject their own commands to an SQL database (Oracle,*

> *MySQL, MariaDB, MSSQL). Through this vulnerability, they can retrieve sensitive data from an affected site's database, including usernames and password hashes.*
>
> *Unauthenticated attacks, like the one seen in this particular SQL Injection vulnerability, are very serious, because they can be automated—making it easy for hackers to mount successful, widespread attacks against vulnerable websites. The number of active installs, the ease of exploitation, and the effects of a successful attack are what makes this vulnerability particularly dangerous.*

PRODSECBUG-2198 is one of more than three dozen security bugs Magento developers disclosed and fixed on Tuesday. It affects the following versions:

- Magento Commerce < 1.14.4.1
- Magento Open Source < 1.9.4.1
- Magento < 2.1.17
- Magento < 2.2.8
- Magento < 2.3.1

Sites that want to quickly protect themselves from this vulnerability only can install a stand-alone patch. Many of the other flaws also pose a threat, but because they generally require a hacker to be authenticated, they aren't considered as severe. To be fully protected against all vulnerabilities, sites will have to upgrade to Magento Commerce or Open Source 2.3.1 or 2.2.8.

Montpas said Magento site administrators can check to see if their site has been targeted in 2198 exploits by checking the access_log file for multiple hits to the following path:

/catalog/product/frontend_action_synchronize

A small number of hits to that path may indicate a legitimate request, but more than a couple dozen hits from the same IP

address in a few minutes should be considered suspicious.

This post was originally published on 3/28/2019, 2:58 PM. It was updated to report that publicly available exploit code was published less than a day later.

https://arstechnica.com/?p=1482917

VMware Patches Flaws Disclosed at Pwn2Own 2019

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/k8FrkR-bb3g/vmware-patches-flaws-disclosed-pwn2own-2019

Critical Flaw Allows Hackers to Take Control of PowerFlex AC Drives

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/mW_2yUPosS4/critical-flaw-allows-hackers-take-control-powerflex-ac-drives

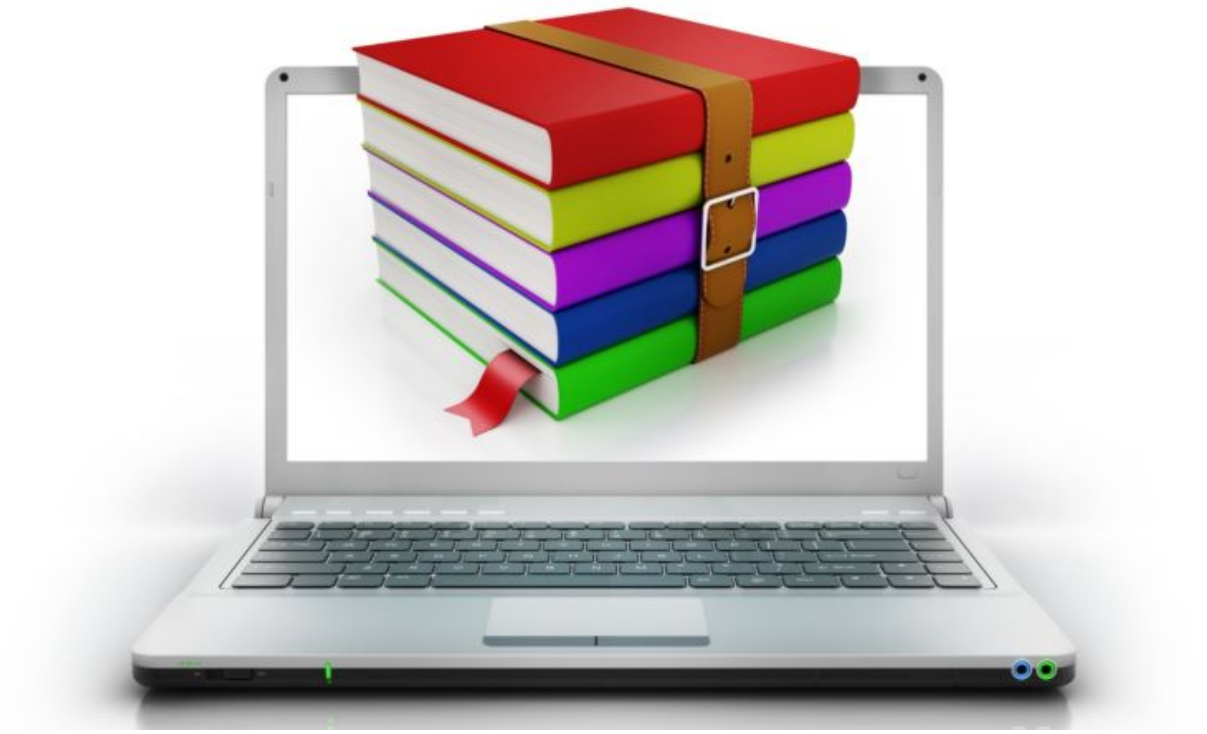
---

WinRAR Vulnerability Exploited to Deliver New Malware

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/_hIciDMeQ9s/winrar-vulnerability-exploited-deliver-new-malware

---

A rogue's gallery of bad actors is exploiting that critical WinRAR flaw



reader comments

54 with 45 posters participating

Share this story

A critical vulnerability in the WinRAR file-compression utility is under active attack by a wide range of bad actors who are exploiting the code-execution flaw to install password stealers and other types of malicious software.

In one campaign, according to a report published by researchers from security firm FireEye, attackers are spreading files that purport to contain stolen data. One file, titled leaks copy.rar, contains email addresses and passwords that were supposedly compromised in a breach. Attackers claim another file, cc.rar, contains stolen credit card data. Other files have names including zabugor.rar, ZabugorV.rar, Combolist.rar, Nulled2019.rar, and IT.rar.

Hidden inside the files are payloads from a variety of different malware families. They include a keylogger known as QuasarRat and malware containing Chinese language text known as Buzy.

The FireEye report identified three other campaigns, including:

- One that impersonates an educational accreditation body that seems to use a PDF letter copied from the website of the Council on Social Work Education as a decoy. When extracted, the RAR file plants a Visual Basic script in the computer's startup folder. The script causes the computer to install a remote-access trojan called Netwire.
- An attack targeting the Israeli military industry that uses decoy files related to SysAid, a helpdesk service based in Israel. A malicious payload, dubbed SappyCache,

will decrypt a file stored in a temporary folder to obtain the address of a command and control channel. SappyCache will then attempt to download and install a second-stage malware file from the server. The server never responded during the FireEye analysis.

- An attack potentially targeting a single person in Ukraine that uses a purported PDF message from the country's former President Viktor Yanukovych. The exploit drops a batch file into the startup folder that, when executed, installed a payload dubbed Empire.

FireEye isn't the only firm that's seeing such exploits. A separate report from security firm Symantec said that an espionage hacking outfit known both as Elfin and APT33 has been spotted exploiting the WinRAR vulnerability against a target in the chemical industry of Saudi Arabia.

Attackers sent a spear-phishing email to at least two employees in the targeted company. The email included a file dubbed JobDetails.rar. If extracted on a computer using a vulnerable version of WinRAR, the attack could install any file of the attackers' choice. Prior to the attack, Symantec updated its software to block exploits. The protection prevented the attack from working against the targeted company.

Adam Meyers, vice president of intelligence at security firm CrowdStrike, told Ars:

> *CrowdStrike tracks Elfin/APT-33 activity with a suspected nexus to the Islamic Republic of Iran under the name REFINED KITTEN. This actor has been involved in espionage operations primarily via spear phishing efforts since at least 2013. We can confirm that recently we have observed them deploying a malware we call PoshC2 targeting the Kingdom of Saudi Arabia using an employment themed lure and the recently disclosed CVE-2018-20250 vulnerability.*

Interestingly, the Symantec report said that an Elfin attack on a US-based organization last February downloaded WinRAR on a compromised machine. Elfin downloaded and utilized WinRAR during their post-compromise attempts to exfiltrate data, Symantec Threat Analyst Sylvester Segura said in an email.

As Ars previously reported, the code-execution vulnerability in WinRAR went unreported for more than 19 years. It's the result of an absolute path traversal flaw that makes it possible for archive files to extract to the Windows startup folder (or any other folder of the archive creator's choosing) without generating a warning. From there, malicious payloads are automatically run the next time the computer reboots. The flaw was fixed in version 5.70. The vulnerability is especially serious, because WinRAR has an installed base of about 500 million, and the software has no means for automatically updating itself.

Two weeks ago, a report emerged that attackers were exploiting the vulnerability to install hard-to-detect malware on vulnerable computers. The new reports indicate that the WinRAR attacks aren't likely to subside any time soon.

"We have seen how various threat actors are abusing the recently disclosed WinRAR vulnerability using customized decoys and payloads, and by using different propagation techniques such as email and URL," FireEye researcher Dileep Kumar Jallepalli wrote. "Because of the huge WinRAR customer-base, lack of auto-update feature, and the ease of exploitation of this vulnerability, we believe this will be used by more threat actors in the upcoming days."

https://arstechnica.com/?p=1482285