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