Magento commerce platform has fixes, users told to install asap

31 March 2019, by Nancy Cohen

Credit: CC0 Public Domain

Patches for an ecommerce platform should be applied immediately. No ifs, maybes, buts, laters. Researchers say anyone using the Magento platform should upgrade as soon as possible and in light of the threat, as soon as possible means right now.

The e-commerce platform Magento has released patches for 37 vulnerabilities, *Threatpost* said on Friday. Magento released four critical patches, four high severity patches and 26 medium severity bugs and three low severity bugs in the patch roundup.

Magento versions impacted were 2.1 prior to 2.1.17, Magento 2.2 prior to 2.2.8 and Magento 2.3 prior to 2.3.1.

Lucian Constantin in *CSO* listed just what types of activities the attackers could perform if exploiting the flaws: remote code execution, SQL injection, cross-site scripting, privilege escalation, information disclosure and spamming.

These included flaws that could have let attackers take over a site and create new admin accounts.

Constantin said Magento, used by thousands of online shops, had security issues affecting both the commercial and open-source versions of its platform.

The latest development is that the Magento platform could soon face attacks after hackers publicly released code that exploits a vulnerability in its systems, said *TechRadar*, which could be used to plant payment card skimmers on sites that have not yet been updated.

Attempts at exploiting e-commerce sites are relentless and this turned out to be a running story. PRODSECBUG-2198 is the name of the SQL injection vulnerability that attackers can exploit without the need for authentication, if attackers attempt an exploit.

KoDDoS wrote about the SQL injection without the need for authentication bug and noted that the Sucuri security firm "said in a blog post that everyone should upgrade immediately if they are using Magento."

Magento's site presented the Magento 2.3.1, 2.2.8 and 2.1.17 update, saying "A SQL injection vulnerability has been identified in pre-2.3.1 Magento code. To quickly protect your store from this vulnerability only, install patch PRODSECBUG-2198. However, to protect against this vulnerability and others, you must upgrade to Magento Commerce or Open Source 2.3.1 or 2.2.8. We strongly suggest that you install these full patches as soon as you can."

How urgent is urgent? Dan Goodin in *Ars Technica* said the newer turn of events made this call-to-patch very urgent.

"Attack code was published on Friday that exploits a critical vulnerability in the Magento e-commerce

platform, all but guaranteeing it will be used to plant payment card skimmers on sites that have yet to install a recently released patch."

Magento is regarded as a popular e-commerce platform. How popular? Jeremy Kirk,*BankInfoSecurity,* noted its reported numbers—$155 billion in commerce in 2018 and more than 300,000 businesses and merchants using the software.

Out of the flaws identified, the most discussed on tech watching sites has been the SQL injection vulnerability.

Sucuri Security talked about the SQL injection issue in Magento Core and warned the bug was critical (CVSS 8.8) and easy to exploit remotely, said *Threatpost*.

(The Common Vulnerability Scoring System framework rates the severity of vulnerabilities, and 10 indicates the most severe.)

Marc-Alexandre Montpas, Sucuri Security researcher, said, "we strongly encourage Magento users to update their sites to the latest version of the branch they are using; either 2.3.1, 2.2.8, or 2.1.17."

For those unfamiliar with the SQL injection, *CSO* last year said there are several types, "but they all involve an attacker inserting arbitrary SQL into a web application database query." It is a type of attack that can give an adversary control over your web application database by inserting arbitrary SQL code into a database query."

Constantin offered a bigger picture view where Magento is just one example of trouble in online shopping land: The number of attacks against online shops in general has increased over the past year, he said, and some of the groups are specialists in web skimming.

TechRadar: "Competing gangs of cybercriminals have spent the last six months trying to infect e-commerce sites with card skimming malware to steal users' payment details." *TechRadar* also pointed out that over 300,000 businesses and merchants used the platform's services.

What's web skimming? The culprits inject "rogue scripts on computers to capture credit card details," as *CSO* put it.

Last year, Adobe had announced agreement to acquire the Magento Commerce platform. The news release described the platform as "built on proven, scalable technology supported by a vibrant community of more than 300,000 developers." The partner ecosystem, said the release, "provides thousands of pre-built extensions, including payment, shipping, tax and logistics."

Jérôme Segura, lead malware intelligence analyst at Malwarebytes, told *Ars Technica* 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."

The groups specialize in slipping payment card skimming malware into sites, said Jeremy Kirk in *BankInfoSecurity*.