Security Leftovers

By Roy Schestowitz
Created 03/12/2021 - 3:42pm
Submitted by Roy Schestowitz on Friday 3rd of December 2021 03:42:46 PM Filed under Security [1]

- **Security updates for Friday [LWN.net]** [2]

  Security updates have been issued by CentOS (krb5 and mailman), Debian (gmp and libread), Fedora (php-symfony4 and wireshark), Mageia (bluez, busybox, docker-container, gfbgraph, hivex, nss, perl/perl-Encode, and udisks2/libblockdev), openSUSE (permissions), Oracle (mailman and mailman:2.1), Red Hat (mailman, mailman:2.1, and nss), Scientific Linux (mailman and nss), and SUSE (nodejs14).

- **New Payment Data Stealing Malware Hides in Nginx Process on Linux Servers** [3]

  E-commerce platforms in the U.S., Germany, and France have come under attack from a new form of malware that targets Nginx servers in an attempt to masquerade its presence and slip past detection by security solutions.

  "This novel code injects itself into a host Nginx application and is nearly invisible," Sansec Threat Research team said in a new report. "The parasite is used to steal data from eCommerce servers, also known as 'server-side Magecart.'"

- **FGKASLR Appears Closer To Mainline For Improving Linux Security** [4]

  Kernel Address Space Layout Randomization has been common on Linux for a decade and a half now while more recently has been Function-Granular (or sometimes referred to as Finer-Grained) KASLR for further upping the security benefits by making it much harder to predict kernel address positions for attacks.
Posted in early 2020 by Intel's Kristen Carlson Accardi was the initial FGKASLR code for improving security. While KASLR helps make memory addresses less predictable, once an attacker determines the base address it's not as effective. Function-Granular/Finer-Grained KASLR applies function-reordering on top of KASLR. The functions are reordered at boot time and thus much harder for attacks relying on known kernel memory locations.

This Week In Security: GoDaddy, Tardigrade, Monox, And BigSig | Hackaday

After the Thanksgiving break, we have two weeks of news to cover, so hang on for an extra-long entry. First up is GoDaddy, who suffered a breach starting on September 6th. According to an SEC filing, they noticed the problem on November 17th, and determined that there was unauthorized access to their provisioning system for their WordPress hosting service. For those keeping track at home, that's two months and eleven days that a malicious actor had access. And what all was compromised? The email address and customer number of the approximate 1.2 million GoDaddy WordPress users; the initial WordPress password, in the clear; the SFTP and database passwords, also in the clear; and for some customers, their private SSL key.

The saving grace is that it seems that GoDaddy's systems are segregated well enough that this breach doesn't seem to have led to further widespread compromise. It's unclear why passwords were stored in the clear beyond the initial setup procedure. To be safe, if you have a WordPress instance hosted by GoDaddy, you should examine it very carefully for signs of compromise, and rotate associated passwords. The SSL keys may be the most troubling, as this would allow an attacker to impersonate the domain. Given the length of time the attack had access, it would not surprise me to learn that more of GoDaddy's infrastructure was actually compromised.

Bangladesh, South African and Iraqi Government sites have been found to be hosting web shells | Netcraft News

Netcraft recently confirmed that a Bangladesh Army site was hosting an Outlook Web Access (OWA) web shell. Additionally, an OWA web shell was found on the Department of Arts and Culture site for the South-African Kwazulu-Natal province and an Iraqi government site was found to be hosting a PHP shell. Web shells are a common tool used by attackers to maintain control of a compromised web server, providing a web interface from which arbitrary commands can be executed on the server hosting the shell. OWA provides remote access to Microsoft Exchange mailboxes; since the disclosure of the ProxyLogon vulnerabilities in March, Microsoft Exchange has become a popular target for cyberattacks.

When using a browser to visit the web shell installed on the Department of Arts and Culture's site, the malicious activity was not immediately obvious, with the shell masquerading as a variable dump. Web shells are often buried in the filesystem alongside benign files, making it difficult for webmasters to detect and take them down. Even after patching the vulnerabilities
used to install a shell, the shell itself also needs to be removed to stop further malicious activity. Sites containing web shells can often remain compromised for long periods of time.

Source URL: http://www.tuxmachines.org/node/158675

Links:
[2] https://lwn.net/Articles/877582/rss