Security: Patches, Core Infrastructure Initiative (CII), Crypto AG, More Issues

By Roy Schestowitz
Created 18/02/2020 - 4:21pm

Security updates for Tuesday [3]

Security updates have been issued by Arch Linux (systemd and thunderbird), Debian (clamav, libgd2, php7.3, spamassassin, and webkit2gtk), Fedora (kernel, kernel-headers, and sway), Mageia (firefox, kernel-linus, mutt, python-pillow, sphinx, thunderbird, and webkit2), openSUSE (firefox, nextcloud, and thunderbird), Oracle (firefox and ksh), Red Hat (curl, java-1.7.0-openjdk, kernel, and ruby), Scientific Linux (firefox and ksh), SUSE (sudo and xen), and Ubuntu (clamav, php5, php7.0, php7.2, php7.3, postgresql-10, postgresql-11, and webkit2gtk).


The Linux Foundation?s Core Infrastructure Initiative (CII), a project that helps support best practices and the security of critical open source software projects, and the Laboratory for Innovation Science at Harvard (LISH), today announced the release of ?Vulnerabilities in the Core,? a Preliminary Report and Census II of Open Source Software.

This Census II analysis and report represent important steps towards understanding and addressing structural and security complexities in the modern day supply chain where open source is pervasive, but not always understood. Census II identifies the most commonly used free and open source software (FOSS) components in production applications and begins to
examine them for potential vulnerabilities, which can inform actions to sustain the long-term security and health of FOSS. Census I (2015) identified which software packages in the Debian Linux distribution were the most critical to the kernel's operation and security.

?The Census II report addresses some of the most important questions facing us as we try to understand the complexity and interdependence among open source software packages and components in the global supply chain,? said Jim Zemlin, executive director at the Linux Foundation. ?The report begins to give us an inventory of the most important shared software and potential vulnerabilities and is the first step to understand more about these projects so that we can create tools and standards that results in trust and transparency in software.?

The malware doesn?t appear to be the first to demand explicit images: In 2017, security firm Kaspersky reported another type of ransomware that demanded nude photos in exchange for unlocking access to infected computers. In other cases, scammers on dating apps have requested nude photos from would-be suitors, then held them for ransom by threatening to leak the photos.

Vulnerabilities that can be hidden away out of sight are amongst the most-coveted by cyber-criminals and spooks alike. That's why zero-day vulnerabilities are deemed so valuable, and cause so much high-level concern when they are exposed. It's also why the CIA secretly purchased an encryption equipment provider to be able to hide backdoors in the products and spy upon more than 100 governments.

While we are almost accustomed to reading government warnings about vulnerabilities in the Windows operating system, Linux cybersecurity threat warnings are less common. Which is partly why this report on the hidden exploit threat within both Linux and Windows systems caught my eye. The Eclypsium researchers concentrated on unsigned firmware as this is a known attack vector, which can have devastating implications, yet one in which vendors have appeared to be slow taking seriously enough. The unsigned firmware in question was found in peripherals used in computers from Dell, Lenovo and HP as well as other major manufacturers. They also demonstrated a successful attack using a network interface card with, you guessed it, unsigned firmware that is used by the big three server manufacturers.

"Despite previous in-the-wild attacks," the report said, "peripheral manufacturers have been
slow to adopt the practice of signing firmware, leaving millions of Windows and Linux systems at risk of firmware attacks that can exfiltrate data, disrupt operations and deliver ransomware."

The truth is that, as far as cybersecurity is concerned, much of the defensive effort is focused on the operating system and applications. Hardly surprising, given these are the most visible attack surfaces. By not adding firmware into the threat prevention model, however, organizations are leaving a gaping hole just waiting to be filled by threat actors. "This could lead to implanted backdoors, network traffic sniffing, data exfiltration, and more," says Katie Teitler, a senior analyst at TAG Cyber. "Unfortunately, though, firmware vulnerabilities can be harder to detect and more difficult to patch," she says, "best practice is to deploy automated scanning for vulnerabilities and misconfigurations at the component level, and continuously monitor for new issues or exploits."

The Week in Internet News: CIA Had Encryption Backdoor for Decades[7]

The U.S. CIA secretly had an ownership stake in Swiss encryption company Crypto AG for decades and was able to read encrypted messages sent using the company's technology, the Washington Post reports. West German intelligence agencies worked with the CIA. Forbes columnist Jody Westby called for a congressional investigation.

Insights from Avast/Jumpshot data: Pitfalls of data anonymization[8]

There has been a surprising development after my previous article on the topic, Avast having announced that they will terminate Jumpshot and stop selling users? data. That's not the end of the story however, with the Czech Office for Personal Data Protection starting an investigation into Avast's practices. I'm very curious to see whether this investigation will confirm Avast's claims that they were always fully compliant with the GDPR requirements. For my part, I now got a glimpse of what the Jumpshot data actually looks like. And I learned that I massively overestimated Avast's success when anonymizing this data.

[...]

The data I saw was an example that Jumpshot provided to potential customers: an excerpt of real data for one week of 2019. Each record included an exact timestamp (milliseconds precision), a persistent user identifier, the platform used (desktop or mobile, which browser), the approximate geographic location (country, city and ZIP code derived from the user's IP address), a guess for user's gender and age group.

What it didn't contain was ?every click, on every site. This data sample didn't belong to the ?All Clicks Feed? which has received much media attention. Instead, it was the ?Limited Insights Pro Feed? which is supposed to merely cover user's shopping behavior: which products they looked at, what they added to the cart and whether they completed the order. All
of that limited to shopping sites and grouped by country (Germany, UK and USA) as well as product category such as Shoes or Men's Clothing.

This doesn't sound like there would be all too much personal data? But there is, thanks to a ?referrer? field being there. This one is supposed to indicate how the user came to the shopping site, e.g. from a Google search page or by clicking an ad on another website. Given the detailed information collected by Avast, determining this referrer website should have been easy?yet Avast somehow failed this task. And so the supposed referrer is typically a completely unrelated random web page that this user visited, and sometimes not even a page but an image or JSON data.

If you extract a list of these referrers (which I did), you see news that people read, their web mail sessions, search queries completely unrelated to shopping, and of course porn. You get a glimpse into what porn sites are most popular, what people watch there and even what they search for. For each user, the ?limited insights? actually contain a tiny slice of their entire browsing behavior. Over the course of a week this exposed way too much information on some users however, and Jumpshot customers watching users over longer periods of time could learn a lot about each user even without the ?All Clicks Feed.?


Byos, Inc., an endpoint security company focused on concept of Endpoint Microsegmentation through Hardware-Enforced Isolation, recommends caution for attendees of major conferences and events such as the RSA Conference 2020, a leading cybersecurity conference in San Francisco, February 24-28, and travelers in general risks of Free Wi-Fi. Many attendees will access the Internet via multiple free Wi-Fi connection points from Hotels, Airports, Coffee Shops and the Conference itself, and every free Wi-Fi access presents security risks for users that Byos calls ?The Dirty Half-Dozen.?

[...]

The Dirty Half-Dozen risks are:

- Scanning, enumerating, and fingerprinting
- Eavesdropping
- Evil-Twin Wi-Fi
- Exploits
- Lateral network infections
- DNS hijacking

Source URL: http://www.tuxmachines.org/node/134214

Links:
