Security updates for Thursday [1]

Security updates have been issued by Debian (gdal), Fedora (nethack), Mageia (okular, sleuthkit, and webkit2), openSUSE (salt), Oracle (icu, kernel, python-pip, python-virtualenv, and zsh), Red Hat (icu, python-imaging, thunderbird, and zsh), Scientific Linux (icu, python-imaging, and zsh), SUSE (postgresql10), and Ubuntu (apache2).

Upcoming Chrome and Chrome OS releases [2]

Due to adjusted work schedules at this time, we are pausing upcoming Chrome and Chrome OS releases. Our primary objectives are to ensure they continue to be stable, secure, and work reliably for anyone who depends on them. We’ll continue to prioritize any updates related to security, which will be included in Chrome 80. Please, follow this blog for updates.

Google Discontinues Chrome And Chrome OS Releases [3]

There seems to be the slightest change in the release date of Chrome and Chrome OS. As reported by Google, They are pausing Chrome and Chrome OS release due to adjusted work schedules.

Eset expands protection for businesses with Endpoint Antivirus for Linux [4]
Eset Endpoint Antivirus for Linux is designed to provide advanced protection from threats to organisations' general desktops. Powered by the advanced Eset LiveGrid technology, the platform combines speed, accuracy and minimal system impact, leaving more system resources for the desktop's vital tasks in order to maintain business continuity, the company said.

The Let's Encrypt certificate revocation scare

The Let's Encrypt project has made real strides in helping to ensure that every web site can use the encrypted HTTPS protocol; it has provided TLS certificates at no charge that are accepted by most or all web browsers. Free certificates accepted by the browsers are something that was difficult to find prior to the advent of the project in 2014; as of the end of February, the project has issued over a billion certificates. But a bug that was recently found in the handling of Certificate Authority Authorization (CAA) by the project put roughly 2.6% of the active certificates—roughly three million—at risk of immediate revocation. As might be expected, that caused a bit of panic in some quarters, but it turned out that the worst outcome was largely averted.

Let's Encrypt allows web-site operators to sign up for its service to sign their TLS certificates, so that browsers will recognize the certificate as valid. Let's Encrypt acts as a Certificate Authority (CA) and its keys are signed by a CA (IdenTrust) that is carried in the root certificate store for the browsers. That means a browser can follow the signature chain from a root certificate it trusts all the way to the certificate of the site, thus establishing the validity of the keys contained in the certificate.

In order for a site to get a certificate from Let's Encrypt, its administrator needs to show that they control the domain in question. That's typically done by adding a challenge value provided by Let's Encrypt to either the DNS information for the domain or via a URL that can be retrieved from the domain's web server. The administrator proves that they have the needed access, thus show that the domain is under their control.

Administrators who wish to restrict the kinds of certificates that can be issued for their domains can add CAA records to their DNS configuration. Those can be used to disallow certain providers, such as Let's Encrypt, from issuing certificates for a domain or portion of one. For example, the web site administrator at "subdomain.example.com" could not receive a certificate from Let's Encrypt or some other CA simply by adding a web page to the server they control if the administrator of the top-level "example.com" domain disallowed that with CAA records. Some sites may also want to restrict the CAs that can be used; some CAs offer services beyond just signing, which may be required for security or regulatory compliance.

Source URL: http://www.tuxmachines.org/node/135381

Links:
[1] https://lwn.net/Articles/815442/rss