New Security Patches and New UEFI 'Secure' Boot Catastrophe

By Roy Schestowitz

Security updates have been issued by Arch Linux (webkit2gtk), CentOS (GNOME, grub2, and kernel), Debian (firefox-esr, grub2, json-c, kdepim-runtime, libapache2-mod-auth-openidc, net-snmp, and xrdp), Gentoo (chromium and firefox), Mageia (podofo), openSUSE (knot and tomcat), Oracle (grub2, kernel, postgresql-jdbc, and python-pillow), Red Hat (firefox, grub2, kernel, and kernel-rt), SUSE (grub2), and Ubuntu (firefox, grub2, grub2-signed, and librsvg).

Grub2 updates for Red Hat systems are making some unbootable

As reported in the comments on the Grub2 secure-boot vulnerabilities report, the updates for grub2 for RHEL 8 and CentOS 8 are making some systems unbootable. The boot problems are seemingly unrelated to whether the system has secure boot enabled. It may be worth waiting a bit for that to shake out.

Servers at risk from ?BootHole? bug ? what you need to know

That’s our tongue-in-cheek name for a cybersecurity vulnerability that not only gets assigned
an identifier like CVE-2020-10713, but also acquires an impressive name plus a jaunty logo (and even, in one intriguing case, a theme tune).

This month’s bug with an impressive name (see what we did there?) is called BootHole, and its logo rather cheekily shows a boot with a worm sticking out of a hole in the toecap.

The bad news is that this bug affects the integrity of bootup process itself, meaning that it provides a way for attackers to insert code that will run next time you restart your device, but during the insecure period after you turn on the power but before the operating system starts up.

The good news for most of us is that it relies on a bug in a bootloader program known as GRUB, short for Grand Unified Boot Loader, which is rarely found on Windows or Mac computers.

Why the GRUB2 Secure Boot Flaw Doesn’t Affect Purism Computers [6]

To understand why this flaw does not affect Purism computers, it helps to understand why UEFI Secure Boot exists to begin with, and how it and the security exploit works. Attacks on the boot process are particularly nasty as they occur before the system’s kernel gets loaded. Attackers who have this ability can then compromise the kernel before it runs, allowing their attack to persist through reboots while also hiding from detection. UEFI Secure Boot is a technology that aims to protect against these kinds of attacks by signing boot loaders like GRUB2 with private keys controlled ultimately by Microsoft. UEFI Firmware on the computer contains the public certificate counterparts for those private keys. At boot time UEFI Secure Boot checks the signatures of the current GRUB2 executable and if they don’t match, it won’t allow the executable to run.

If you’d like to understand the GRUB2 vulnerability in more detail, security journalist Dan Goodin has a great write-up at Ars Technica. In summary, an attacker can trigger a buffer overflow in GRUB2 as it parses the grub.cfg configuration file (this file contains settings for the GRUB2 menu including which kernels to load and what kernel options to use). This buffer overflow allows the attacker to modify GRUB2 code in memory and execute malicious code of their choice, bypassing the protection UEFI Secure Boot normally would have to prevent such an attack.

Unfortunately, UEFI Secure Boot doesn’t extend its signature checks into configuration files like grub.cfg. This means you can change grub.cfg without triggering Secure Boot and the attack exploited that limitation to modify grub.cfg in a way that would then exploit the running GRUB2 binary after it had passed the signature check.

Further complicating the response to this vulnerability is the fact that it’s not enough to patch GRUB2. Because the vulnerable GRUB2 binaries have already been signed by Microsoft’s certificate, an attacker could simply replace a patched GRUB2 with the previous, vulnerable version. Patching against this vulnerability means updating your UEFI firmware (typically
using reflashing tools and firmware provided by your vendor) so that it can add the vulnerable
GRUB2 binary signatures to its overall list of revoked signatures.