EXPLAINER: The security flaw that's freaked out the internet

December 15 2021, by Frank Bajak

Lydia Winters shows off Microsoft's "Minecraft" built specifically for HoloLens at the Xbox E3 2015 briefing before Electronic Entertainment Expo, June 15, 2015, in Los Angeles. Security experts around the world raced Friday, Dec. 10, 2021, to patch one of the worst computer vulnerabilities discovered in years, a critical flaw in open-source code widely used across industry and government in cloud services and enterprise software. Cybersecurity experts say users of the online game Minecraft have already exploited it to breach other users by pasting a short message into in a chat box. Credit: AP Photo/Damian Dovarganes, File

Security pros say it's one of the worst computer vulnerabilities they've ever seen. Firms including Microsoft say state-backed Chinese and Iranian hackers and rogue cryptocurrency miners have already seized on it.

The Department of Homeland Security has sounded a dire alarm, ordering federal agencies to urgently find and patch bug instances because it's so easily exploitable—and telling those with public-facing networks to put up firewalls if they can't be sure. A small piece of code, the affected software often undocumented.

Lodged in an extensively used utility called Log4j, the flaw lets internet-based attackers easily seize control of everything from industrial control systems to web servers and consumer electronics. Simply identifying which systems use the utility is a challenge; it is often hidden under layers of other software.

The top U.S. cybersecurity defense official, Jen Easterly, deemed the flaw "one of the most serious I've seen in my entire career, if not the most serious" in a call Monday with state and local officials and partners in the private sector. Publicly disclosed last Thursday, it's catnip for cybercriminals and digital spies because it allows easy, password-free entry.

The Cybersecurity and Infrastructure Security Agency, or CISA, which Easterly runs, stood up a resource page Tuesday to deal with the flaw it says is present in hundreds of millions of devices. Other heavily computerized countries were taking it just as seriously, with Germany activating its national IT crisis center.

A wide swath of critical industries, including electric power, water, food and beverage, manufacturing and transportation, were exposed, said Dragos, a top cybersecurity firm. "I think we won't see a single major

software vendor in the world—at least on the industrial side—not have a problem with this," said Sergio Caltagirone, the company's vice president of threat intelligence.

Eric Goldstein, who heads CISA's cybersecurity division, said no federal agencies were known to have been compromised. But these are early days.

"What we have here is a extremely widespread, easy to exploit and potentially highly damaging vulnerability that certainly could be utilized by adversaries to cause real harm," he said.

A SMALL PIECE OF CODE, A WORLD OF TROUBLE

The affected software, written in the Java programming language, logs user activity. Developed and maintained by a handful of volunteers under the auspices of the open-source Apache Software Foundation, it is highly popular with commercial software developers. It runs across many platforms—Windows, Linux, Apple's macOS—powering everything from web cams to car navigation systems and medical devices, according to the security firm Bitdefender.

Goldstein told reporters in a Tuesday evening call that CISA would be updating an inventory of patched software as fixes become available. "We expect remediation will take some time," he said.

Apache Software Foundation said the Chinese tech giant Alibaba notified it of the flaw on Nov. 24. It took two weeks to develop and release a fix.

Beyond patching, computer security pros have an even more daunting challenge: trying to detect whether the vulnerability was exploited—whether a network or device was hacked. That will mean

weeks of active monitoring. A frantic weekend of trying to identify—and slam shut—open doors before hackers exploited them now shifts to a marathon.

LULL BEFORE THE STORM

"A lot of people are already pretty stressed out and pretty tired from working through the weekend—when we are really going to be dealing with this for the foreseeable future, pretty well into 2022," said Joe Slowik, threat intelligence lead at the network security firm Gigamon.

The cybersecurity firm Check Point said Tuesday it detected more than half a million attempts by known malicious actors to identify the flaw on corporate networks across the globe. It said the flaw was exploited to install cryptocurrency mining malware—which uses computing cycles to mine digital money surreptitiously—in five countries.

As yet, no successful ransomware infections leveraging the flaw have been detected, though Microsoft said in a blog post that criminals who break into networks and sell access to ransomware gangs had been detected exploiting the vulnerability in both Windows and Linux systems. It said criminals were also rapidly incorporating the vulnerability into botnets that corral multiple zombie computers for larcenous ends.

"I think what's going to happen is it's going to take two weeks before the effect of this is seen because hackers got into organizations and will be figuring out what to do to next." John Graham-Cumming, chief technical officer of Cloudflare, whose online infrastructure protects websites from online threats.

Senior researcher Sean Gallagher of the cybersecurity firm Sophos said we're in the lull before the storm.

"We expect adversaries are likely grabbing as much access to whatever they can get right now with the view to monetize and/or capitalize on it later on." That would include extracting usernames and passwords.

State-backed Chinese and Iranian state hackers were already leveraging the vulnerability for espionage, said Microsoft and the cybersecurity firm Mandiant. Microsoft said North Korean and Turkish state-backed hackers were, too. John Hultquist, a top Mandiant analyst wouldn't name targets but said the Iranian actors are "particularly aggressive" and had taken part in ransomware attacks against Israel primarily for disruptive ends.

Microsoft said the same Chinese cyberspy group that exploited a flaw in its on-premises Exchange Server software in early 2021 were using Log4j to "extend their typical targeting."

SOFTWARE: INSECURE BY DESIGN?

The Log4j episode exposes a poorly addressed issue in software design, experts say. Too many programs used in critical functions have not been developed with enough thought to security.

Open-source developers like the volunteers responsible for Log4j should not be blamed so much as an entire industry of programmers who often blindly include snippets of such code without doing due diligence, said Slowik of Gigamon.

Popular and custom-made applications often lack a "Software Bill of Materials" that lets users know what's under the hood—a crucial need at times like this.

"This is becoming obviously more and more of a problem as software vendors overall are utilizing openly available software," said Caltagirone

of Dragos.

In industrial systems particularly, he added, formerly analog systems in everything from water utilities to food production have in the past few decades been upgraded digitally for automated and remote management. "And one of the ways they did that, obviously, was through software and through the use of programs which utilized Log4j," Caltagirone said.