Global race to patch critical computer bug

December 10 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 experts around the world raced Friday 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.

"I'd be hard-pressed to think of a company that's not at risk," said Joe Sullivan, chief security officer for Cloudflare, whose online infrastructure protects websites from malicious actors. Untold millions of servers have it installed, and experts said the fallout would not be known for several days.

New Zealand's computer emergency response team was among the first to report that the flaw in a Java-language utility for Apache servers used to log user activity was being "actively exploited in the wild" just hours after it was publicly reported Thursday and a patch released.

The vulnerability, dubbed 'Log4Shell,' was rated 10 on a scale of one to 10, the worst possible. Anyone with the exploit can get full acces s to an unpatched machine.

"The internet's on fire right now. People are scrambling to patch and there are script kiddies and all kinds of people scrambling to exploit it," said Adam Meyers, senior vice president of intelligence at the cybersecurity firm Crowdstrike. "In the last 12 hours it has been fully weaponized."

The vulnerability in the Apache Software Foundation module was discovered Nov. 24 by the Chinese tech giant Alibaba, the foundation said. Meyers expected computer emergency response teams to have a busy weekend trying to identify all impacted machines. The hunt is complicated by the fact that affected software can be in programs provided by third parties.

The flaw's exploitation was apparently first discovered in Minecraft, an online game hugely popular with kids and owned by Microsoft.

Meyers and security expert Marcus Hutchins said Minecraft users had already been using it to execute programs on the computers of other users by pasting a short message in a chat box.

Microsoft said it had issued a software update for Minecraft users and "customers who apply the fix are protected."

Researchers reported finding evidence the vulnerability could be exploited in servers run by companies including Apple, Amazon, Twitter and Cloudflare.

Cloudflare's Sullivan said there we no indication his company's servers had been compromised. Apple, Amazon and Twitter did not immediately respond to requests for comment.

Citation: Global race to patch critical computer bug (2021, December 10) retrieved 9 April 2024 from https://techxplore.com/news/2021-12-global-patch-critical-bug.html