

Microsoft comes under blistering criticism for “grossly irresponsible” security

reader comments

75 with

Microsoft has once again come under blistering criticism for the security practices of Azure and its other cloud offerings, with the CEO of security firm Tenable saying Microsoft is “grossly irresponsible” and mired in a “culture of toxic obfuscation.”

The comments from Amit Yoran, chairman and CEO of Tenable, come six days after Sen. Ron Wyden (D-Ore.) blasted Microsoft for what he said were “negligent cybersecurity practices” that enabled hackers backed by the Chinese government to steal hundreds of thousands of emails from cloud customers, including officials in the US Departments of State and Commerce. Microsoft has yet to provide key details about the mysterious breach, which involved the hackers obtaining an extraordinarily powerful encryption key granting access to a variety of its other cloud services. The company has taken pains ever since to obscure its infrastructure’s role in the mass breach.

Critics pile on

On Wednesday, Yoran took to LinkedIn to castigate Microsoft for failing to fix what the company said on Monday was a “critical” issue that gives hackers unauthorized access to data and apps managed by Azure AD, a Microsoft cloud offering for managing user authentication inside large organizations. Monday’s disclosure said that the firm notified Microsoft of the problem in March and that Microsoft reported 16 weeks later that it had been fixed. Tenable researchers told Microsoft that the fix was incomplete. Microsoft set the date for providing a complete fix to September 28.

“To give you an idea of how bad this is, our team very quickly discovered authentication secrets to a bank,” Yoran wrote. “They were so concerned about the seriousness and the ethics of the issue that we immediately notified Microsoft.” He continued:

Advertisement

Did Microsoft quickly fix the issue that could effectively lead to the breach of multiple customers’ networks and services? Of course not. They took more than 90 days to implement a partial fix—and only for new applications loaded in the service.

A Microsoft representative said Microsoft didn’t immediately have a comment in response to Yoran’s post. Responding to Wyden’s letter last week, Microsoft brushed off the criticisms, saying: “This incident demonstrates the evolving challenges of cybersecurity in the face of sophisticated attacks. We continue to work directly with government agencies on this issue, and maintain our commitment to continue sharing information at Microsoft Threat Intelligence blog.”

Tenable is discussing the issue in only general terms to prevent malicious hackers from learning how to actively

exploit it in the wild. In an email, company officials said: "There is a vulnerability that provides access to the Azure fabric, at the very least. Once the details of this vulnerability are known, exploitation is relatively trivial. It is for this reason that we are withholding all technical details." While Yoran's post and Tenable's disclosure avoid the word vulnerability, the email said the term is accurate.

The post came on the same day that security firm Sygnia disclosed a set of what it called "vectors" that could be leveraged following a successful breach of an Azure AD Connect account. The vectors allow attackers to intercept credentials via man-in-the-middle attacks or to steal cryptographic hashes of passwords by injecting malicious code into a hash syncing process. Code injection could also allow attackers to gain a persistent presence inside the account with a low probability of being detected.

"The default configuration exposes clients to the described vectors only if privileged access was gained to the AD Connect server," Ilia Rabinovich, director of adversarial tactics at Sygnia, wrote in an email. "Therefore, a threat actor needs to perform preliminary steps before proceeding with the exploitation process of the vectors."

Advertisement

Both Tenable and Sygnia said that the security vulnerabilities or vectors they disclosed weren't related to the recent attack on Microsoft cloud customers.

Serious cybersecurity defects

In last week's letter to the heads of the Justice Department, Federal Trade Commission, and the Cybersecurity and Infrastructure Security Agency, Wyden accused Microsoft of hiding its role in the 2020 SolarWinds supply chain attack, which Kremlin hackers used to infect 18,000 customers of the network management software. A subset of those customers,

including nine federal agencies and 100 organizations, received follow-on attacks that breached their networks.

The senator went on to pin blame on Microsoft for the recent mass breach of the Departments of State and Commerce and the other Azure customers. Specific failings, Wyden said, included Microsoft having “a single skeleton key that, when inevitably stolen, could be used to forge access to different customers’ private communications.” He also faulted Microsoft for waiting five years to refresh the signing key abused in the attacks, saying best practices are to rotate keys more frequently. He also criticized the company for allowing authentication tokens signed by an expired key, as was the case in the attack.

“While Microsoft’s engineers should never have deployed systems that violated such basic cybersecurity principles, these obvious flaws should have been caught by Microsoft’s internal and external security audits,” Wyden wrote. “That these flaws were not detected raises questions about what other serious cybersecurity defects these auditors also missed.”

In Wednesday’s post, Yoran voiced largely the same criticisms.

“What you hear from Microsoft is ‘just trust us,’ but what you get back is very little transparency and a culture of toxic obfuscation,” he wrote. “How can a CISO, board of directors or executive team believe that Microsoft will do the right thing given the fact patterns and current behaviors? Microsoft’s track record puts us all at risk. And it’s even worse than we thought.”

<https://arstechnica.com/?p=1958508>