A single text is all it took to unleash code-execution worm in Cisco Jabber

reader comments

51 with 41 posters participating

Share this story

Until Wednesday, a single text message sent through Cisco's Jabber collaboration application was all it took to touch off a self-replicating attack that would spread malware from one Windows user to another, researchers who developed the exploit said.

The wormable attack was the result of several flaws, which Cisco patched on Wednesday, in the Chromium Embedded Framework that forms the foundation of the Jabber client. A filter that's designed to block potentially malicious content in incoming messages failed to scrutinize code that invoked a programming interface known as "onanimationstart."

Jumping through hoops

But even then, the filter still blocked content that contained <style>, an HTML tag that had to be included in a malicious payload. To bypass that protection, the researchers used code that was tailored to a built-in animation component called spinner-grow. With that, the researchers were able to achieve a cross-site scripting exploit that injected a malicious payload directly into the internals of the browser built into

Jabber.

A security sandbox built into the Chromium Embedded Framework, or CEF, would normally store the payload in a container that's isolated from sensitive parts of the app. To work around this constraint, the researchers abused the window.CallCppFunction, which is designed to open files sent by other Cisco Jabber users. By manipulating a function parameter that accepts files, the researchers were able to break out of the sandbox.

"Since Cisco Jabber supports file transfers, an attacker can initiate a file transfer containing a malicious .exe file and force the victim to accept it using an XSS attack," researchers from security firm Watchcom Security wrote in a post. "The attacker can then trigger a call to window.CallCppFunction, causing the malicious file to be executed on the victim's machine."

Computer worms are among the most potent types of malware attack because a single strike can touch off a chain of follow-on damage, in much the way toppling a domino causes thousands of dominos behind it to fall. When the wormable attack achieves remote code execution—as is the case here—worms are the most severe. Fixes from Cisco come as more businesses are relying on video conferencing to conduct everyday work.

Accordingly, CVE-2020-3495, the designation assigned to the Cisco Jabber vulnerability, has a severity rating of 9.9 out of a maximum 10 based on the Common Vulnerability Scoring System. Cisco's advisory has more details here.

More code execution

The Watchcom researchers devised a separate code-execution attack that exploited a different vulnerability. That one worked by abusing Cisco Jabber protocol handlers, which help the operating system know what to do when a user clicks on a

URL containing a Jabber-specific protocol.

The researchers explained:

> *These protocol handlers are vulnerable to command injection because they fail to consider URLs that contain spaces. By including a space in the URL, an attacker can inject arbitrary command line flags that will be passed to the application. Since the application uses CEF and accepts Chromium command line flags, several flags that can be used to execute arbitrary commands or load arbitrary DLLs exist. An example of such a flag is –GPU-launcher. This flag specifies a command that will be executed when CEFs GPU process is started.*
>
> *This vulnerability can be combined with the XSS vulnerability to achieve code execution without transferring any files to the victim. This makes it possible to deliver malware without writing any files to disk, thus bypassing most antivirus software.*

The video below demonstrates the proof-of-concept exploit they developed.

[embedded content]
Cisco Jabber Exploit Demo—discovered by Watchcom Security Group.
CVE-2020-3430 carries a severity score of 8.8.

Two other vulnerabilities—CVE-2020-3537 and CVE-2020-3498—have severity ratings of 5.7 and 6.5, respectively.

The vulnerabilities affect Cisco Jabber for Windows versions 12.1 through 12.9.1. People using vulnerable versions should update as soon as possible.

https://arstechnica.com/?p=1703578

Hackers are exploiting a critical flaw affecting >350,000 WordPress sites

reader comments

58 with 41 posters participating

Share this story

Hackers are actively exploiting a vulnerability that allows them to execute commands and malicious scripts on Websites running File Manager, a WordPress plugin with more than 700,000 active installations, researchers said on Tuesday. Word of the attacks came a few hours after the security flaw was patched.

Attackers are using the exploit to upload files that contain webshells that are hidden in an image. From there, they have a convenient interface that allows them to run commands in plugins/wp-file-manager/lib/files/, the directory where the File Manager plugin resides. While that restriction prevents hackers from executing commands on files outside of the directory, hackers may be able to exact more damage by uploading scripts that can carry out actions on other parts of a vulnerable site.

NinTechNet, a website security firm in Bangkok, Thailand, was among the first to report the in-the-wild attacks. The post

said that a hacker was exploiting the vulnerability to upload a script titled hardfork.php and then using it to inject code into the WordPress scripts /wp-admin/admin-ajax.php and /wp-includes/user.php.

Backdooring vulnerable sites at scale

In email, NinTechNet CEO Jerome Bruandet wrote:

> *It's a bit too early to know the impact because when we caught the attack, hackers were just trying to backdoor websites. However, one interesting thing we noticed is that attackers were injecting some code to password-protect the access to the vulnerable file (connector.minimal.php) so that other groups of hackers could not exploit the vulnerability on the sites that were already infected.*
>
> *All commands can be run in the /lib/files folder (create folders, delete files etc), but the most important issue is that they can upload PHP scripts into that folder too, and then run them and do whatever they want to the blog.*
>
> *So far, they are uploading "FilesMan", another file manager often used by hackers. This one is heavily obfuscated. In the next few hours and days we'll see exactly what they will do, because if they password-protected the vulnerable file to prevent other hackers to exploit the vulnerability it is likely they are expecting to come back to visit the infected sites.*

Fellow website security firm Wordfence, meanwhile, said in its own post that it had blocked more than 450,000 exploit attempts in the past few days. The post said that the attackers are trying to inject various files. In some cases, those files were empty, most likely in an attempt to probe for vulnerable sites and, if successful, inject a malicious file

later. Files being uploaded had names including hardfork.php, hardfind.php, and x.php.

“A file manager plugin like this would make it possible for an attacker to manipulate or upload any files of their choosing directly from the WordPress dashboard, potentially allowing them to escalate privileges once in the site’s admin area,” Chloe Chamberland, a researcher with security firm Wordfence, wrote in Tuesday’s post. “For example, an attacker could gain access to the admin area of the site using a compromised password, then access this plugin and upload a webshell to do further enumeration of the server and potentially escalate their attack using another exploit.”

52% of 700,000 = potential for damage

The File Manager plugin helps administrators manage files on sites running the WordPress content management system. The plugin contains an additional file manager known as elFinder, an open source library that provides the core functionality in the plugin, along with a user interface for using it. The vulnerability arises from the way the plugin implemented elFinder.

“The core of the issue began with the File Manager plugin renaming the extension on the elFinder library’s connector.minimal.php.dist file to .php so it could be executed directly, even though the connector file was not used by the File Manager itself,” Chamberland explained. “Such libraries often include example files that are not intended to be used ‘as is’ without adding access controls, and this file had no direct access restrictions, meaning the file could be accessed by anyone. This file could be used to initiate an elFinder command and was hooked to the elFinderConnector.class.php file.”

The developers of File Manager credited researches Ville Korhonen and Seravo with discovering and first reporting the vulnerability. The researchers, who said they found the vulnerability as part of their regular “WordPress upkeep service,” published their own writeup here.

Sal Aguilar, a contractor who sets up and secures WordPress sites, took to Twitter to warn of attacks he’s seeing.

“Oh crap!!!” he wrote. “The WP File Manager vulnerability is SERIOUS. Its spreading fast and I’m seeing hundreds of sites getting infected. Malware is being uploaded to /wp-content/plugins/wp-file-manager/lib/files.”

The security flaw is in File Manager versions ranging from 6.0 to 6.8. Statistics from WordPress show that currently about 52 percent of installations are vulnerable. With more than half of File Manager’s installed base of 700,000 sites vulnerable, the potential for damage is high. Sites running any of these versions should updated to 6.9 as soon as possible.

Updated to add fourth-to-last paragraph.

https://arstechnica.com/?p=1702887

Attackers are trying to exploit a high-severity zeroday in Cisco gear

reader comments

35 with 25 posters participating, including story author

Share this story

Telecoms and data-center operators take note: attackers are actively trying to exploit a high-severity zeroday vulnerability in Cisco networking devices, the company warned over the weekend.

The security flaw resides in Cisco's iOS XR Software, an operating system for carrier-grade routers and other networking devices used by telecommunications and data-center providers. In an advisory published on Saturday, the networking-gear manufacturer said that a patch is not yet available and provided no timeline for when one would be released.

Memory exhaustion

CVE-2020-3566, as the vulnerability is tracked, allows attackers to "cause memory exhaustion, resulting in instability of other processes" including but not limited to interior and exterior routing protocols. Exploits work by sending maliciously crafted Internet Group Management Protocol traffic. Normally, IGMP communications are used by one-to-many networking applications to conserve resources when streaming video and related content. A flaw in the way iOS XR Software queues IGMP packets makes it possible to consume memory resources.

"An attacker could exploit this vulnerability by sending crafted IGMP traffic to an affected device," Saturday's advisory stated. "A successful exploit could allow the attacker to cause memory exhaustion, resulting in instability of other processes. These processes may include, but are not limited to, interior and exterior routing protocols."

Independent researcher Troy Mursch, who monitors active Internet attacks using honeypots—or simulated production networks belonging to organizations and consumers—told me he had seen limited signs of exploitation attempts.

“There was some IGMP scanning activity last week, but we haven’t seen a widespread type of attack,” he said.

He said the most likely purpose of the attacks would be to cause denial of services that, by definition, prevent the intended use of products, often to huge swaths of the Internet.

DVMRP

Attacks have the potential to be severe because they threaten high-availability servers where reliability and security are paramount. To be vulnerable, a device must be configured to accept traffic that uses DVMRP, short for the Distance Vector Multicast Routing Protocol. Networks use DVMRP to share information between routers in the transport of IP multicast packets. Networks that have no need of DVMRP often turn it off.

Cisco didn’t elaborate on what the attacks were doing beyond saying they could exhaust memory that would disrupt various processes. Cisco also didn’t say if any of the exploit attempts are succeeding. The company rated the severity of the vulnerability “high” with a Common Vulnerability Scoring System tally of 8.6 out of a total of 10. The IGMP packet-queuing flaw resides in the Distance Vector Multicast Routing Protocol folded into iOS XR.

The advisory provides indicators that users can check to look for evidence they’re under attack. The document says there are no workarounds available to use until a patch can be installed. It does, however, list things administrators can do to mitigate the effects.

https://arstechnica.com/?p=1702472

Snapdragon chip flaws put >1 billion Android phones at risk of data theft

reader comments

125 with 91 posters participating

Share this story

A billion or more Android devices are vulnerable to hacks that can turn them into spying tools by exploiting more than 400 vulnerabilities in Qualcomm’s Snapdragon chip, researchers reported this week.

The vulnerabilities can be exploited when a target downloads a video or other content that’s rendered by the chip. Targets can also be attacked by installing malicious apps that require no permissions at all.

From there, attackers can monitor locations and listen to nearby audio in real time and exfiltrate photos and videos. Exploits also make it possible to render the phone completely unresponsive. Infections can be hidden from the operating system in a way that makes disinfecting difficult.

Snapdragon is what’s known as a system on a chip that provides

a host of components, such as a CPU and a graphics processor. One of the functions, known as digital signal processing, or DSP, tackles a variety of tasks, including charging abilities and video, audio, augmented reality, and other multimedia functions. Phone makers can also use DSPs to run dedicated apps that enable custom features.

New attack surface

“While DSP chips provide a relatively economical solution that allows mobile phones to provide end users with more functionality and enable innovative features—they do come with a cost,” researchers from security firm Check Point wrote in a brief report of the vulnerabilities they discovered. “These chips introduce new attack surface and weak points to these mobile devices. DSP chips are much more vulnerable to risks as they are being managed as ‘Black Boxes’ since it can be very complex for anyone other than their manufacturer to review their design, functionality or code.”

Qualcomm has released a fix for the flaws, but so far it hasn’t been incorporated into the Android OS or any Android device that uses Snapdragon, Check Point said. When I asked when Google might add the Qualcomm patches, a company spokesman said to check with Qualcomm. The chipmaker didn’t respond to an email asking.

Check Point is withholding technical details about the vulnerabilities and how they can be exploited until fixes make their way into end-user devices. Check Point has dubbed the vulnerabilities Achilles. The more than 400 distinct bugs are tracked as CVE-2020-11201, CVE-2020-11202, CVE-2020-11206, CVE-2020-11207, CVE-2020-11208 and CVE-2020-11209.

In a statement, Qualcomm officials said: “Regarding the Qualcomm Compute DSP vulnerability disclosed by Check Point, we worked diligently to validate the issue and make appropriate mitigations available to OEMs. We have no evidence

it is currently being exploited. We encourage end users to update their devices as patches become available and to only install applications from trusted locations such as the Google Play Store.”

Check Point said that Snapdragon is included in about 40 percent of phones worldwide. With an estimated 3 billion Android devices, that amounts to more than a billion phones. In the US market, Snapdragons are embedded in around 90 percent of devices.

There’s not much helpful guidance to provide users for protecting themselves against these exploits. Downloading apps only from Play can help, but Google’s track record of vetting apps shows that advice has limited efficacy. There’s also no way to effectively identify boobytrapped multimedia content.

https://arstechnica.com/?p=1697639

Hackers actively exploit high-severity networking vulnerabilities

reader comments

31 with 27 posters participating

Share this story

Hackers are actively exploiting two unrelated high-severity vulnerabilities that allow unauthenticated access or even a complete takeover of networks run by Fortune 500 companies and government organizations.

The most serious exploits are targeting a critical vulnerability in F5's Big-IP advanced delivery controller, a device that's typically placed between a perimeter firewall and a Web application to handle load balancing and other tasks. The vulnerability, which F5 patched three weeks ago, allows unauthenticated attackers to remotely run commands or code of their choice. Attackers can then use their control of the device to hijack the internal network it's connected to.

Prescient

The presence of a remote code execution flaw in a device located in such a sensitive part of a network gave the vulnerability a maximum severity rating of 10. Immediately after F5 released a patch on June 30, security practitioners predicted that the flaw—which is tracked as CVE-2020-5902—would be exploited against any vulnerable networks that didn't quickly install the update. On Friday, the US Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory that proved those warnings prescient.

"CISA has conducted incident response engagements at US Government and commercial entities where malicious cyber threat actors have exploited CVE-2020-5902—an RCE vulnerability in the BIG-IP Traffic Management User Interface (TMUI)—to take control of victim systems," the advisory stated.

Officials continued:

> *CISA has observed scanning and reconnaissance, as well as*

> *confirmed compromises, within a few days of F5's patch release for this vulnerability. As early as July 6, 2020, CISA has seen broad scanning activity for the presence of this vulnerability across federal departments and agencies—this activity is currently occurring as of the publication of this Alert.*
>
> *CISA has been working with several entities across multiple sectors to investigate potential compromises relating to this vulnerability. CISA has confirmed two compromises and is continuing to investigate. CISA will update this Alert with any additional actionable information.*

Et tu, Cisco?

Attackers are exploiting a second vulnerability found in two network products sold by Cisco. Tracked as CVE-2020-3452, the path-traversal flaw resides in the company's Adaptive Security Appliance and Firepower Threat Defense systems. It allows unauthenticated people to remotely view sensitive files that, among other things, can disclose WebVPN configurations, bookmarks, Web cookies, partial Web content, and HTTP URLs. Cisco issued a patch on Wednesday. A day later, it updated its advisory.

"Cisco has become aware of the availability of public exploit code and active exploitation of the vulnerability that is described in this advisory," the update said. "Cisco encourages customers with affected products to upgrade to a fixed release as soon as possible."

Proof-of-concept code began circulating almost immediately after Cisco issued the fix, setting off a race between attackers and defenders.

The impact of these vulnerabilities—particularly the one affecting F5 customers—is serious. These in-the-wild attacks

provide ample reason to occupy the weekend of any IT administrators who have yet to patch their vulnerable systems.

https://arstechnica.com/?p=1694402

Microsoft urges patching severe-impact, wormable server vulnerability

Enlarge / A data center stock photo. I spy with my little eye some de-badged EMC Symmetrix DMX-3 or DMX-4 disk bays at right and some de-badged EMC CX disk bays at left. Disk arrays like these are a mainstay of traditional enterprise data center SANs.

reader comments

39 with 25 posters participating, including story author

Share this story

Microsoft is urgently advising Windows server customers to patch a vulnerability that allows attackers to take control of entire networks with no user interaction and, from there, rapidly spread from computer to computer.

The vulnerability, dubbed SigRed by the researchers who discovered it, resides in Windows DNS, a component that automatically responds to requests to translate a domain into the IP address computers need to locate it on the Internet. By

sending maliciously formed queries, attackers can execute code that gains domain administrator rights and, from there, take control of an entire network. The vulnerability, which doesn't apply to client versions of Windows, is present in server versions from 2003 to 2019. SigRed is formally tracked as CVE-2020-1350. Microsoft issued a fix as part of this month's Update Tuesday.

Both Microsoft and the researchers from Check Point, the security firm that discovered the vulnerability, said that it's wormable, meaning it can spread from computer to computer in a way that's akin to falling dominoes. With no user interaction required, computer worms have the potential to propagate rapidly just by virtue of being connected and without requiring end users to do anything at all.

When a worm's underlying vulnerability easily allows malicious code to be executed, exploits can be especially pernicious, as was the case with both the WannaCry and NotPetya attacks from 2016 that shut down networks worldwide and caused billions of dollars in damage.

Check Point researchers said that the effort required to exploit SigRed was well within the means of skilled hackers. While there's no evidence that the vulnerability is actively under exploit at the moment, Check Point said that's likely to change, and if it does, the destructive effects would be high.

In a technical analysis, Sagi Tzadik, the company researcher who found the vulnerability in May and privately reported it to Microsoft, wrote:

> *We believe that the likelihood of this vulnerability being exploited is high, as we internally found all of the primitives required to exploit this bug. Due to time constraints, we did not continue to pursue the exploitation of the bug (which includes chaining together all of the exploitation primitives), but we do believe that a determined*

> *attacker will be able to exploit it. Successful exploitation of this vulnerability would have a severe impact, as you can often find unpatched Windows Domain environments, especially Domain Controllers. In addition, some Internet Service Providers (ISPs) may even have set up their public DNS servers as WinDNS.*

In a brief writeup here, Microsoft analysts agreed the underlying heap-based buffer overflow was wormable. The company also rated the chances of exploitation as "more likely". Many outside researchers concurred.

"If I've understood the article correctly, calling it 'wormable' is actually an understatement," Vesselin Vladimirov Bontchev, a security expert who works for the National Laboratory of Computer Virology in Bulgaria, wrote on Twitter. "It's suitable for flash worms a la Slammer, which infected the whole population of vulnerable computers on the Internet in something like 10 minutes flat."

> *It's suitable for flash worms a la Slammer, which infected the whole population of vulnerable computers on the Internet in something like 10 minutes flat.*
>
> *— Vess (@VessOnSecurity) July 14, 2020*

Bontchev was disagreeing with fellow security researcher Marcus Hutchins, who said he thought it was more likely attackers would exploit SigRed in an attempt to wage crippling ransomware campaigns. In that scenario, attackers would take control of a network's DNS server and then use it to push malware to all connected client computers. Slammer is a reference to SQL Slammer, a worm from 2003 that exploited two vulnerabilities in Microsoft's SQL Server. Within 10 minutes of being activated, SQL Slammer infected more than 75,000 machines, some of them belonging to Microsoft.

Organizations that use Windows DNS should carefully assess the risks and install Tuesday’s patch as soon as possible. For those who can’t patch immediately, Microsoft offered stopgap measures people can take in the write up linked above.

https://arstechnica.com/?p=1691743

Unscheduled fixes for critical Windows flaws delivered through rare channel

reader comments

9 with 8 posters participating

Share this story

Microsoft has published unscheduled fixes for two critical vulnerabilities that make it possible for attackers to execute malicious code on computers running any version of Windows 10.

Unlike the vast majority of Windows patches, the ones released on Tuesday were delivered through the Microsoft Store. The normal channel for operating System security fixes is Windows Update. Advisories here and here said users need not take any action to automatically receive and install the fixes.

“Affected customers will be automatically updated by Microsoft Store. Customers do not need to take any action to receive the update,” both advisories said. “Alternatively, customers who want to receive the update immediately can check for updates with the Microsoft Store App; more information on this process can be found here.”

When I checked both the Microsoft Store and the Windows Update on my Windows 10 laptop, however, I saw no confirmation the patch had been installed. Normally, Windows 10 users can use the Windows Update tab within the Update and Security settings section to ensure patches have been installed. The link provided in the advisories offered no clarity. Microsoft representatives didn’t immediately respond to questions for this post.

Both vulnerabilities reside in Windows code libraries that manage codecs used to render images or other multimedia content. Attackers can exploit the flaws to execute code of their choice or to obtain information stored on vulnerable systems. Exploits can be delivered in specially designed image files that corrupt computer memory. Presumably, the images could be delivered on compromised websites a target visits or when targets open a malicious file sent by email. Tuesday’s advisories didn’t say if exploits worked only when targets opened the malformed images in specific apps or any app.

Microsoft credited Abdul-Aziz Hariri of Trend Micro’s Zero Day Initiative with discovering and privately reporting the bugs. Both advisories indicate that there’s no evidence of the flaw being actively exploited in the wild. With no clear way to verify the patches have been installed, Windows 10 users for now will have to take Microsoft’s word that they’re automatically installed. This post will be updated if Microsoft answers questions I sent.

https://arstechnica.com/?p=1688847

Intel will soon bake anti-malware defenses directly into its CPUs

Enlarge / A mobile PC processor code-named Tiger Lake. It will be the first CPU to offer a security capability known as Control-Flow Enforcement Technology.

reader comments

71 with 49 posters participating

Share this story

The history of hacking has largely been a back-and-forth game, with attackers devising a technique to breach a system, defenders constructing a countermeasure that prevents the technique, and hackers devising a new way to bypass system security. On Monday, Intel is announcing its plans to bake a new parry directly into its CPUs that’s designed to thwart software exploits that execute malicious code on vulnerable computers.

Control-Flow Enforcement Technology, or CET, represents a fundamental change in the way processors execute instructions from applications such as Web browsers, email clients, or PDF readers. Jointly developed by Intel and Microsoft, CET is designed to thwart a technique known as return-oriented programming, which hackers use to bypass anti-exploit measures software developers introduced about a decade ago. While Intel

first published its implementation of CET in 2016, the company on Monday is saying that its Tiger Lake CPU microarchitecture will be the first to include it.

ROP, as return-oriented programming is usually called, was software exploiters' response to protections such as Executable Space Protection and address space layout randomization, which made their way into Windows, macOS, and Linux a little less than two decades ago. These defenses were designed to significantly lessen the damage software exploits could inflict by introducing changes to system memory that prevented the execution of malicious code. Even when successfully targeting a buffer overflow or other vulnerability, the exploit resulted only in a system or application crash, rather than a fatal system compromise.

ROP allowed attackers to regain the high ground. Rather than using malicious code written by the attacker, ROP attacks repurpose functions that benign applications or OS routines have already placed into a region of memory known as the stack. The "return" in ROP refers to use of the RET instruction that's central to reordering the code flow.

Very effective

Alex Ionescu, a veteran Windows security expert and VP of engineering at security firm CrowdStrike, likes to say that if a benign program is like a building made of Lego bricks that were built in a specific sequence, ROP uses the same Lego pieces but in a different order. In so doing, ROP converts the building into a spaceship. The technique is able to bypass the anti-malware defenses because it uses memory-resident code that's already permitted to be executed.

CET introduces changes in the CPU that create a new stack called the control stack. This stack can't be modified by attackers and doesn't store any data. It stores the return addresses of the Lego bricks that are already in the stack.

Because of this, even if an attacker has corrupted a return address in the data stack, the control stack retains the correct return address. The processor can detect this and halt execution.

“Because there is no effective software mitigation against ROP, CET will be very effective at detecting and stopping this class of vulnerability,” Ionescu told me. “Previously, operating systems and security solutions had to guess or infer that ROP had happened, or perform forensic analysis, or detect the second stage payloads/effect of the exploit.”

Not that CET is limited to defenses against ROP. CET provides a host of additional protections, some of which thwart exploitation techniques known as jump-oriented programming and call-oriented programming, to name just two. ROP, however, is among the most interesting aspects of CET.

Those who do not remember the past

Intel has built other security functions into its CPUs with less-than-stellar results. One is Intel’s SGX, short for Software Guard eXtension, which is supposed to carve out impenetrable chunks of protected memory for security-sensitive functions such as the creation of cryptographic keys. Another security add-on from Intel is known as the Converged Security and Management Engine, or simply the Management Engine. It’s a subsystem inside Intel CPUs and chipsets that implements a host of sensitive functions, among them the firmware-based Trusted Platform Module used for silicon-based encryption, authentication of UEFI BIOS firmware, and the Microsoft System Guard and BitLocker.

A steady stream of security flaws discovered in both CPU-resident features, however, has made them vulnerable to a variety of attacks over the years. The most recent SGX vulnerabilities were disclosed just last week.

It’s tempting to think that CET will be similarly easy to defeat, or worse, will expose users to hacks that wouldn’t be possible if the protection hadn’t been added. But Joseph Fitzpatrick, a hardware hacker and a researcher at SecuringHardware.com, says he’s optimistic CET will perform better. He explained:

> *One distinct difference that makes me less skeptical of this type of feature versus something like SGX or ME is that both of those are “adding on” security features, as opposed to hardening existing features. ME basically added a management layer outside the operating system. SGX adds operating modes that theoretically shouldn’t be able to be manipulated by a malicious or compromised operating system. CET merely adds mechanisms to prevent normal operation—returning to addresses off the stack and jumping in and out of the wrong places in code—from completing successfully. Failure of CET to do its job only allows normal operation. It doesn’t grant the attacker access to more capabilities.*

Once CET-capable CPUs are available, the protection will work only when the processor is running an operating system with the necessary support. Windows 10 Version 2004 released last month provides that support. Intel still isn’t saying when Tiger Lake CPUs will be released. While the protection could give defenders an important new tool, Ionescu and fellow researcher Yarden Shafir have already devised bypasses for it. Expect them to end up in real-world attacks within the decade.

https://arstechnica.com/?p=1683807

Exploit code for wormable flaw on unpatched Windows devices published online

reader comments

33 with 22 posters participating

Share this story

A researcher has published exploit code for a Microsoft Windows vulnerability that, when left unpatched, has the potential to spread from computer to computer with no user interaction.

So-called wormable security flaws are among the most severe, because the exploit of one vulnerable computer can start a chain reaction that rapidly spreads to hundreds of thousands, millions, or tens of millions of other vulnerable machines. The WannaCry and NotPetya exploits of 2017, which caused worldwide losses in the billions and tens of billions of dollars respectively, owe their success to CVE-2017-0144, the tracking number for an earlier wormable Windows vulnerability.

Also key to the destruction was reliable code developed by and later stolen from the National Security Agency and finally published online. Microsoft patched the flaw in March 2017, two months before the first exploit took hold.

Puppies will die

Proof-of-concept exploit code for the new wormable Windows

vulnerability was published on Monday by a Github user with the handle Chompie1337. The exploit isn't reliable and frequently results in crashes that present a BSOD, shorthand for the "blue screen of death" Windows displays during system failures. Regardless, the code still serves as a blueprint that, with more work, could be used to remotely compromise vulnerable machines and then spread.

"This has not been tested outside of my lab environment," the Github user wrote. "It was written quickly and needs some work to be more reliable. Sometimes you BSOD. Using this for any purpose other than self education is an extremely bad idea. Your computer will burst in flames. Puppies will die."

SMBGhost, the name given to the new Microsoft vulnerability, is likely not as easy to exploit by remote attackers, but its potential for wormable exploits and the slow rate of patching even critical security flaws have still stoked concerns among some security professionals. Microsoft has said that the chances of malicious exploits are "more likely."

Like the flaw exploited by WannaCry and NotPetya, it resides in the Windows implementation of the Server Message Block, a service used by operating systems to share files, printers, and other resources on local networks and over the Internet. Like the older flaw, the newer one can be remotely exploited simply by sending maliciously crafted packets to a SMB port connected to the Internet.

Tracked as CVE-2020-0796, the flaw resides in Windows 10 versions 1903 and 1909 and in Windows Server versions 1903 and 1909 if they haven't been patched. All are relatively new OS releases, and Microsoft has invested huge amounts of resources hardening them against precisely these types of attacks. Up until now, researchers have only been able to exploit the bug locally, meaning once they have already gained limited access in a network. By contrast, the ability to use exploits to gain RCE, short for remote code execution, have proved much more

elusive.

“This is probably because remote kernel exploitation is very different from local exploitation in that an attacker can’t utilize useful OS functions such as creating userland processes, referring to PEB [Process Environment Block], and issuing system calls,” researchers from Ricerca Security wrote in a detailed post published in April. “Accompanied with mitigations introduced in Windows 10, this limitation makes the achievement of RCE much more challenging.”

The result of the newly released exploit is that it increases the chances of attackers developing worms that work remotely.

Laggard, patch thyself

Reports of the vulnerability were disclosed and then quickly depublished by security firm Fortinet and Cisco security group Talos on March 10, the regularly scheduled Update Tuesday for that month. No one ever explained why the flaw details were released and then pulled. Two days later, Microsoft issued an unscheduled update that patched the vulnerability.

“We recommend customers install updates as soon as possible as publicly disclosed vulnerabilities have the potential to be leveraged by bad actors,” Microsoft officials wrote in a statement on Friday. “An update for this vulnerability was released in March, and customers who have installed the updates, or have automatic updates enabled, are already protected.”

Workarounds that mitigate exploits but don’t actually fix the underlying vulnerability include:

- Disabling SMB compression
- Blocking port 445

As the world learned from WannaCry and NotPetya, Windows users often wait months or longer to install critical software

updates. Sometimes, the inaction is the result of inattention, but often it’s because patches break core functions inside a network. Still other times it’s because operators aren’t at liberty to shut down their systems for the length of time required to install the patch and make changes to incompatible components or services.

Independent researcher Troy Mursch said he has been seeing “opportunistic mass scanning” for the vulnerability, an indication that attackers have been scoping out vulnerable networks. With reliable exploits looking more likely, now would be a good time for laggards to finally install the patch.

https://arstechnica.com/?p=1681718

Google fixes Android flaws that allow code execution with high system rights

reader comments

45 with 35 posters participating

Share this story

Google has shipped security patches for dozens of vulnerabilities in its Android mobile operating system, two of which could allow hackers to remotely execute malicious code

with extremely high system rights.

In some cases, the malware could run with highly elevated privileges, a possibility that raises the severity of the bugs. That's because the bugs, located in the Android System component, could enable a specially crafted transmission to execute arbitrary code within the context of a privileged process. In all, Google released patches for at least 34 security flaws, although some of the vulnerabilities were present only in devices available from manufacturer Qualcomm.

Anyone with a mobile device should check to see if fixes are available for their device. Methods differ by device model, but one common method involves either checking the notification screen or clicking Settings > Security > Security update. Unfortunately, patches aren't available for many devices.

Two vulnerabilities ranked as critical in Google's June security bulletin are indexed as CVE-2020-0117 and CVE-2020-8597. They're among four System flaws located in the Android system (the other two are ranked with a severity of high). The critical vulnerabilities reside in Android versions 8 through the most recent release of 11.

"These vulnerabilities could be exploited through multiple methods such as email, web browsing, and MMS when processing media files," an advisory from the Department of Homeland Security-funded Multi-State-Information Sharing and Analysis Center said. "Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights."

Vulnerabilities with a severity rating of high affected the Android media framework, the Android framework, and the Android kernel. Other vulnerabilities were contained in components shipped in devices from Qualcomm. The two Qualcomm-

specific critical flaws reside in closed source components. The severity of other Qualcomm flaws were rated as high.

https://arstechnica.com/?p=1680681