Cisco pays $8.6 million for selling surveillance system it knew was vulnerable

reader comments

28 with 27 posters participating

Share this story

Cisco is paying $8.6 million to settle claims that it sold a video-surveillance product the company knew made federal and state agencies vulnerable to serious hacking attacks. This is believed to be the first time a company has made a payout under a federal whistleblower lawsuit alleging failure to have adequate security protections.

The settlement stems from a Video Surveillance Manager package Cisco sold, starting more than a decade ago, to a raft of government agencies. These agencies include the Department of Homeland Security, the Secret Service, the Department of Defense Biometrics Taskforce, the Federal Emergency Management Agency, NASA, the Army, the Navy, the Air Force, and the Marine Corps. Known as VSM, the surveillance package was also used by government agencies in at least 15 states, including New York and California.

A 2011 lawsuit unsealed on Wednesday alleged that Cisco knowingly sold VSM to customers even after learning of a critical vulnerability. This vulnerability allowed hackers to spy on video footage in real time, turn cameras on or off, delete footage, and tamper with locks and other physical

security systems connected on the same network. The lawsuit was filed under the False Claims Act in the US District Court for the Western District of New York. The act allows individuals with inside knowledge to bring suits on behalf of the government when they believe a contractor is committing fraud.

The individual suing Cisco is James Glenn, who was working for a Cisco partner in 2008 when he discovered the vulnerability and privately reported it. In 2010—about a year after being laid off in a cost-cutting measure—Glenn found that the vulnerability still hadn't been fixed. He filed the complaint a year later. Cisco didn't fix the vulnerability until July 2013, more than four years after Glenn made the private report.

"Security disasters"

"The Cisco VSM is fundamentally flawed, leading it to create significant security flaws in any system into which it is incorporated," the complaint alleged. "These flaws are so significant that it would be difficult to correct them sufficiently to bring the product into compliance with federal purchasing standards, even if Cisco fully disclosed the flaws to government purchasers. Because Cisco has deliberately refused to disclose these flaws to government purchasers, the vast majority of all such systems sold to government customers remain in their vulnerable state—a wide network of security disasters waiting to happen."

In a statement, Cisco officials wrote: "We are pleased to have resolved a 2011 dispute involving the architecture of a video-security technology product we added to our portfolio through the Broadware acquisition in 2007. There was no allegation or evidence that any unauthorized access to customers' video occurred as a result of the architecture."

Cisco's statement didn't explain why the company took more

than four years to fix the critical vulnerability or why it continued to sell the package without disclosing the flaw.

The settlement is likely the first payout in a False Claim Act involving a security vulnerability in a product. According to a spokesman for the law firm representing Glenn, most of the $8.6 million award will go to federal and state governments, and more than $1 million will go to Glenn.

https://arstechnica.com/?p=1544671

---

200 million devices—some mission-critical—vulnerable to remote takeover

reader comments

43 with 35 posters participating

Share this story

About 200 million Internet-connected devices—some that may be controlling elevators, medical equipment, and other mission-critical systems—are vulnerable to attacks that give attackers complete control, researchers warned on Monday.

In all, researchers with security firm Armis identified 11 vulnerabilities in various versions of VxWorks, a slimmed-down operating system that runs on more than 2 billion devices

worldwide (this section of Wikipedia's article on the OS lists some of its more notable uses). Billed collectively as Urgent 11, the vulnerabilities consist of six remote code flaws and five less-severe issues that allow things like information leaks and denial-of-service attacks. None of the vulnerabilities affects the most recent version of VxWorks—which was released last week—or any of the certified versions of the OS, including VxWorks 653 or VxWorks Cert Edition.

High stakes

For the 200 million devices Armis estimated are running a version that's susceptible to a serious attack, however, the stakes may be high. Because many of the vulnerabilities reside in the networking stack known as IPnet, they can often be exploited by little more than boobytrapped packets sent from the Internet. Depending on the vulnerability, exploits may also be able to penetrate firewalls and other types of network defenses. The most dire scenarios are attacks that chain together multiple exploits that trigger the remote takeover of multiple devices.

"Such vulnerabilities do not require any adaptations for the various devices using the network stack, making them exceptionally easy to spread," Armis researchers wrote in a technical overview. "In most operating systems, such fundamental vulnerabilities in the crucial networking stacks have become extinct, after years of scrutiny unravelled and mitigated such flaws."

In a post published Monday, Arlen Baker, chief security architect of VxWorks-maker Wind River, wrote:

> *The IPnet networking stack is a component of some versions of VxWorks, including end-of-life (EOL) versions back to 6.5. Specifically, connected devices leveraging older standard VxWorks releases that include the IPnet stack are impacted by*

> *one or more of the discovered vulnerabilities. The latest release of VxWorks is not affected by the Urgent/11 vulnerability, nor are any of Wind River's safety-critical products that are designed for safety certification, such as VxWorks 653 and VxWorks Cert Edition used in critical infrastructure.*

Baker said Wind River researchers believe the number of affected devices is lower than the 200 million estimate provided by Armis. Affected devices, he said, are primarily non-critical devices such as modems, routers, and printers, as well as some industrial and medical devices that reside at the perimeter of organizations' networks and are exposed to the Internet.

Wind River issued patches last month and is in the process of notifying affected customers of the threat. The challenge for many of these customers will be locating the devices on their networks and taking them off-line so they can be updated. Often organizations rely on the devices to run continuously.

The more immediate challenge for organizations that use affected or potentially affected equipment will be to assess the risk they face. Armis researchers are presenting Urgent 11 as posing a serious and imminent threat, potentially at the scale of the Windows vulnerabilities that allowed the 2016 WannaCry worm to sow worldwide disruptions. Armis researchers are also warning that the difficulty of patching the flaws means this risk may be with us for the foreseeable future.

But the threat may very well be much smaller than that assessment. What's more (assuming the threat is as bad as Armis says it is), it may be possible to mitigate the risk through means other than patching, such as access control lists, which restrict the devices that can connect to a vulnerable device. A better mitigation still is to remove a vulnerable device from the outside Internet altogether. Either

way, people inside any organization using devices running VxWorks should make it a priority to do a deep dive on Urgent 11 so they can understand the risk it poses.

https://arstechnica.com/?p=1542997

Whitehats use DoS attack to score key victory against ransomware crooks

Enlarge / A diagram showing how a DoS shut down an ongoing ransomware campaign.

reader comments

21 with 14 posters participating

Share this story

Whitehats used a novel denial-of-service hack to score a key victory against ransomware criminals. Unfortunately, the blackhats have struck back by updating their infrastructure, leaving the fight with no clear winner.

Researchers at security firm Intezer performed the DoS technique against ransomware dubbed QNAPCrypt, a largely undetected strain that, as its name suggests, infects network storage devices made by Taiwan-based QNAP Systems and possibly other manufacturers. The hack spread by exploiting secure shell, (or SSH) connections that used weak passwords. The

researchers' analysis found that each victim received a unique bitcoin wallet for sending ransoms, a measure that was most likely intended to prevent the attackers from being traced. The analysis also showed that QNAPCrypt only encrypted devices after they received the wallet address and a public RSA key from the command-and-control server.

Intezer researchers soon noticed two key weaknesses in that process:

1. The list of bitcoin wallets was created in advance, and it was static, meaning there was a finite number of wallets available, and
2. The attackers' infrastructure didn't perform any authentication on devices that connected and claimed to be infected

The weaknesses allowed the researchers to write a script that could emulate an unlimited number of simulated infections. After spoofing infections for nearly 1,100 devices from 15 separate campaigns, the whitehats exhausted the supply of unique bitcoin wallets the attackers had pre-generated. As a result, the campaigns were disrupted, since devices are only encrypted after they receive the wallet. The image above this post shows how the DoS worked.

"Attackers (and malware developers) are eventually like any other developers, and sometimes they have design flaws, exactly like in this case," Ari Eitan, Intezer's VP of research, wrote in an email. "We took advantage of it as defenders. As far as we know, no one did this type of DoS operation in the past."

The empire strikes back

The ransomware developers responded by updating their code to include the wallets and RSA key inside the executable file that gets delivered to targeted machines. This

“connectionless” payload, as Intezer researchers called it, allowed the attackers to defeat the DoS, but it came at a cost—they had to walk away from their earlier campaigns.

While the QNAPCrypt operators have lived to fight another day, the whitehats scored another small victory. The updated implant shares almost identical code with Linux.Rex, a ransomware strain that was first spotted in 2016 infecting Drupal servers in ransomware and DDoS operations. That gives Intezer and other defenders new insights and intelligence in defeating a ransomware strain that, so far, has gone largely undetected. Intezer has more details here.

https://arstechnica.com/?p=1534219

D-Link agrees to new security monitoring to settle FTC charges

reader comments

31 with 28 posters participating

Share this story

Router and webcam maker D-Link has agreed to implement a new security program to settle charges it failed to safeguard its hardware against well-known and preventable hacks and misrepresented its existing security regimen.

Tuesday’s agreement settles a 2017 complaint by the US Federal Trade Commission that alleged D-Link left thousands of customers open to potentially costly hack attacks. The hardware maker, the FTC said, failed to test its gear against security flaws ranked among the most critical and widespread by the Open Web Application Security Project. The 2017 suit also said that, despite the lack of testing and hardening of its products, D-Link misrepresented its security regimen as reasonable.

Specific shortcomings cited by the FTC included:

- hard-coded login credentials on its D-Link camera software that used easily guessed passwords
- storing mobile app login credentials in human-readable text on a user’s mobile device
- expressly or implicitly describing its hardware as being secure from unauthorized access

and

- repeatedly failing to take reasonable testing and remediation measures to protect hardware from well-known and easily preventable software security flaws

“We sued D-Link over the security of its routers and IP cameras, and these security flaws risked exposing users’ most sensitive personal information to prying eyes,” Andrew Smith, director of the FTC’s Bureau of Consumer Protection, said in a release. “Manufacturers and sellers of connected devices should be aware that the FTC will hold them to account for failures that expose user data to risk of compromise.”

Tuesday’s settlement requires D-Link to implement a security program that better ensures the company’s cameras and routers are secure. The program requires “implementing security planning, threat modeling, testing for vulnerabilities before releasing products, ongoing monitoring to address security flaws, and automatic firmware updates, as well as accepting

vulnerability reports from security researchers.”

Over the next decade, D-Link will also be required every two years to obtain independent third-party assessments of its software security program. Documents related to the assessment must be provided to FTC employees upon request. The settlement also requires the assessor to identify specific evidence for its findings rather than solely relying on assertions by D-Link management. The FTC has the authority to approach the third-party assessor chosen by D-Link.

In the 30 months that have passed since the FTC sued D-Link, hackers have continued to capitalize on past missteps the hardware maker has made. In June 2018, malicious hackers behind the Satori Internet-of-things botnet started mass-exploiting a critical code-execution vulnerability in D-Link hardware that was used by subscribers of Verizon and other ISPs. A month later came word criminals had stolen a D-Link code-signing certificate and were using it to pass off malware that steals passwords and backdoors PCs. A month after that, hackers exploited a vulnerability in D-Link routers that sent users to a fake banking website that attempted to steal their login credentials.

Tuesday’s settlement comes a little more than three years after the FTC settled charges with ASUS over the security of its routers.

https://arstechnica.com/?p=1531161

In-the-wild Mac malware kept

busy in June—here’s a rundown

reader comments

6 with 6 posters participating

Share this story

June was a busy month for Mac malware with the active circulation of at least six threats, several of which were able to bypass security protections Apple has built into modern versions of its macOS.

The latest discovery was published Friday by Mac antivirus provider Intego, which disclosed malware dubbed OSX/CrescentCore that’s available through Google search results and other mainstream channels. It masquerades as an updater or installer for Adobe’s Flash media player, but it’s in fact just a persistent means for its operators to install malicious Safari extensions, rogue disk cleaners, and potentially other unwanted software.

“The team at Intego has observed OSX/CrescentCore in the wild being distributed via numerous sites,” Intego’s Joshua Long wrote of two separate versions of the malware his company has found. “Mac users should beware that they may encounter it, even via seemingly innocuous sources such as Google search results.”

Security evasions

Long said that the CrescentCore versions he observed were signed with certificates belonging to an Apple-trusted developer. That would allow the malware to bypass Gatekeeper,

a macOS protection that's designed to thwart malware by allowing only digitally signed applications to be installed. Both recovered versions of CrescentCore are signed by certificates assigned to a developer using the name Sanela Lovic using certificate fingerprints 5UA7HW48Y7 and D4AYX8GHJS.

Long said he reported the certificate abuse to Apple, but as early Friday afternoon, a tool called WhatsYourSign, developed by Mac security expert Patrick Wardle, showed both signing certificates remained valid. On Friday evening, the tool showed one certificate had been revoked and another remained valid.

CrescentCore uses other techniques to avoid detection and analysis. After targets click on the fake Flash installer/updater, it first checks to see if it's about to be installed inside a virtual machine or on a Mac that's running AV software. If either of those possibilities turns out to be true, the trojan will simply exit and not do anything more. Security researchers almost always test suspected malware inside VMs to prevent accidentally infecting trusted work computers.

Mac users who want to check for infections should look for files with the name Player.dmg (or Player #.dmg or Player (#).dmg where # is a numeral such as 1 or 2) downloaded to the Downloads folder. Infected Macs may also contain folders or files with the following names:

- /Library/com.apple.spotlight.Core
- /Library/Application Support/com.apple.spotlight.Core
- /Library/LaunchAgents/com.google.keystone.plist
- com.player.lights.extensions.appex

Friday's Intego post lists one of at least six macOS threats that have come to light this month. Others include:

- A cryptocurrency miner dubbed LoudMiner by ESET

and Bird Miner by Malwarebytes, the two firms that independently discovered it. The miners, found in a cracked installer for the high-end music production software Ableton Live, work by emulating Linux.

- Malware dubbed OSX/Newtab, which tries to inject tabs into the Safari browser. Some of the file names disguise themselves as government forms or recipe apps. All samples have an identifier of com.NTAppStubInstaller and were digitally signed with the Apple Developer ID cosmina beteringhe (HYC4353YBE).
- Backdoors dubbed NetWire and Mokes that were installed in in-the-wild attacks exploiting a pair of potent Firefox zerodays to target people involved with cryptocurrencies. Both backdoors were able to bypass Gatekeeper and were undetected by antivirus engines at the time the attacks went live.

The recent activity is an indication that more and more malware developers are finding it worth their time to create malicious wares for macOS, a platform they largely shunned a decade ago.

As is the case with Windows computers, the best way to protect Macs against malware is to ensure the OS, browsers, and browser extensions are updated as soon as possible after security patches are released. Another key safeguard is to never run a stand-alone version of Flash (the one built into Chrome is generally OK).

https://arstechnica.com/?p=1529441

Some Medtronic Insulin Pumps Vulnerable to Hacker Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/6wWgjyVc5Bg/some-medtronic-insulin-pumps-vulnerable-hacker-attacks

---

US Cyber Attack on Iran: Search to Exploit Flaw

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/fK2ZjNTTP5U/us-cyber-attack-iran-search-exploit-flaw

---

New ransomware infections are the worst drive-by attacks in recent memory

reader comments

50 with 41 posters participating

Share this story

An ongoing operation that’s installing ransomware and other malware on the computers of unsuspecting website visitors is one of the most potent drive-by attack campaigns researchers have seen in recent memory.

The attacks install three pieces of malware using an exploit kit called GreenFlash Sundown, which researchers identified in 2015 and have continued to follow since. Attacks in recent weeks have spiked again as ShadowGate—one of the names given to the hacker group behind the campaign—has unleashed a highly revamped version of the exploit kit on hacked ad servers run by Web publishers. The most notable compromise is of an ad server belonging to onlinevideoconverter[.]com, a site with more than 200 million visitors per month that converts YouTube videos into video files that can be stored on a computer hard drive.

“They are ongoing and with a scale we haven’t seen in a couple of years when it comes to exploit kit-related attacks,” Jérôme Segura, a Malwarebytes researcher tracking the campaign, said of the attacks on onlinevideoconverter[.]com visitors. “We literally noticed a huge spike in our telemetry starting a few days ago, which is very unusual. Given what we see in our telemetry, this is the most successful drive-by campaign we have seen in quite a while, so we can infer many people were affected by it.”

A significant escalation

Segura reported the revived campaign on Wednesday in a post that said the attacks were one of the first times the attackers had actively targeted people in Europe and North

America. Previously, he said, the group had largely limited attacks to South Korea.

In an analysis published Thursday, researchers from Trend Micro echoed the assessment that the new campaign represents a significant escalation by the once-regional group.

“This is the most notable activity we have seen from this group since 2016,” Trend Micro’s Joseph C. Chen wrote. “Despite their low profile over the past couple of years, it seems that they have been continuously developing and evolving their exploit kit.”

Among the innovations in the new kit: well-obfuscated JavaScript hidden inside a fake GIF image that redirects people to fastimage[.]site, one of the attacker-controlled sites used to serve the exploit code. Another improvement is a fingerprinting mechanism that works on multiple levels to carefully select a subset of visitors to be exploited.

The first level of fingerprinting is performed at the network level. It filters out devices visiting from IP addresses assigned to virtual private networks and similar services, to ensure only users of residential IPs are targeted. Another round of fingerprinting uses a PowerShell script to gather details about the visitors’ devices, including their operating system, user name, video card, hard disk, and any antivirus products.

Crypto is hard

Yet another recently added feature is the use of public key encryption to protect the payloads carried by their exploit. Before targets are infected, the exploits generate a secret key that’s unique to each computer. The secret key is encrypted with a public key and sent to the attackers. The attackers then use the decrypted secret key to encrypt the payloads. In theory, because the secret key is supposed to

reside only in the memory of the targeted computer—and never written to disk or transmitted in plaintext—it should be hard for people reverse-engineering the exploits to analyze or identify the payloads.

Trend Micro researchers were able to defeat the encryption by exploiting a crucial weakness. A cryptographic nonce used in the generation of the unique secret key was reused as a separate encryption key and was sent in plaintext when the targeted computer communicated with one of the attacker servers. Once Trend Micro researchers obtained the nonce, they were able to reproduce the secret key that allowed them to decrypt the payload, or at least parts of it.

The ongoing compromise of onlinevideoconverter[.]com is one of a series of attacks researchers from both Malwarebytes and Trend Micro have observed the group carrying out on self-hosted ad servers running Revive Adversever. (This is an open rsource package that sometimes goes by its old name OpenX Source.)

Representatives of onlinevideoconverter[.]com didn’t respond to an email seeking comment for this post.

The best way to protect against this campaign is to be sure to keep browsers, browser add-ons, and operating systems updated, since the attackss this group is known to use almost always exploit known vulnerabilities for which patches are available. Antivirus protection is also effective, since most engines detect both the exploits and the payloads. Additionally, it’s almost never a bad idea to uninstall stand-alone versions of Flash.

Segura said the campaign is installing three separate pieces of malware, including the SEON ransomware, botnet malware known as Pony, and software that mines cryptocurrency on infected computers. The ransomware is particularly pernicious, since it deletes any shadowcopy files used for backup. The

exploits are currently targeting only Windows computers that run outdated versions of Adobe’s Flash media player. Segura said visitors who have been infected will know immediately.

“The ransomware payload is the indication you were infected,” he told Ars. “It pops up a ransom note, and indeed, all the files have been encrypted.”

https://arstechnica.com/?p=1528735

Many Potential Backdoors Found in Huawei Equipment: Study

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/CBmxUm_OAlI/many-potential-backdoors-found-huawei-equipment-study

---

Chrome OS 75 Adds More Mitigations for Intel MDS Flaws

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/A4r0lSyXCeA/chrome-os-75-adds-more-mitigations-intel-mds-flaws