Researcher Drops 3 Separate 0-Day Windows Exploits in 24 Hours

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/8C78ApK9ksU/researcher-drops-3-separate-0-day-windows-exploits-24-hours

---

PoC Exploits Created for Wormable Windows RDS Flaw

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/caeeIsSwf4I/poc-exploits-created-wormable-windows-rds-flaw

---

Serial publisher of Windows 0-days drops exploits for 3 more unfixed flaws

reader comments

30 with 24 posters participating

Share this story

A serial publisher of Microsoft zeroday vulnerabilities has dropped exploit code for three more unpatched flaws, marking the seventh time the unknown person has done so in the past year.

Technical details of the vulnerabilities, along with working proof-of-concept exploits, are the work of someone using the moniker SandBoxEscaper. A local privilege-escalation vulnerability in the Windows Task Scheduler that was disclosed on Tuesday allows an authenticated attacker to gain SYSTEM privileges on an affected system. On Thursday, the person released a privilege escalation code that exploits a bug in the Windows Error Reporting service. Attackers can use it to modify files that would normally be off limits. A third exploit, which was also released Wednesday, works against Internet Explorer 11 and allows attackers to execute a JavaScript that runs with higher system access than is normally permitted by the browser sandbox.

Decent deal

Like the other exploits SandboxEscaper has published over the past year—including this one Ars covered last August and this one from last October—the three recent ones don’t allow attackers to remotely execute malicious code. Still, as security defenses in recent versions of Windows and other operating systems have improved, the value of these types of exploits has grown, since they are often the only way to bypass security sandboxes and similar protections. Despite some limitations in the exploit that were transparently noted by SandBoxEscaper, the disclosures are significant if they

work as purported against fully patched versions of Windows 10.

“Any new privilege escalation on native Windows 10 is a pretty decent deal as most vulnerabilities are on applications that you put on top of the OS rather than in the OS itself,” Charles Dardaman, a security researcher in Dallas, told Ars. “If an attacker had an RCE or some other way, like phishing, that gave low-level access to a machine, they could then use one of these attacks to escalate to Admin.”

In March, Google reported that a then-unpatched privilege-escalation vulnerability in older versions of Windows was being used alongside an unrelated exploit in the Chrome browser. On its own, neither exploit was able to do much damage, thanks to the defense-in-depth mitigations built into Windows and Chrome. Together, however, the exploits allowed hackers to remotely execute malware of their choice. Dardaman said that the two privilege-escalation vulnerabilities SandboxEscaper published over the past 24 hours are likely to have similar capabilities when combined with the right additional exploit.

In Tuesday’s disclosure, SandboxEscaper wrote that the Task Scheduler vulnerability works by exploiting a flaw in the way the Task Scheduler processes changes to discretionary access control list permissions for an individual file. An advisory published Wednesday by US Cert confirmed that the exploit worked against both 32-bit and 64-bit versions of Windows 10.

Below is video of the exploit in action:

> *Here’s a demo of a Windows 10 privilege escalation zeroday that US Cert has confirmed works against Windows 10. Microsoft has yet to comment on it. pic.twitter.com/hFP05fqPRM*
>
> *— Dan Goodin (@dangoodin001) May 22, 2019*

Microsoft representatives have yet to comment on the disclosures this week, and researchers have yet to confirm the two exploits published Wednesday work against fully-patched Windows 10. Given SandboxEscaper's track record, people should assume the exploits work as billed and stay apprised of any new updates or bulletins that may be published in the coming days.

https://arstechnica.com/?p=1509701

Critical Vulnerabilities Plague South Korean ActiveX Controls

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/4JoWmmWL62Q/critical-vulnerabilities-plague-south-korean-activex-controls

---

Flaw Exposes Mitsubishi PLCs to Remote DoS Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/YhozS8xdgvQ/flaw-exposes-mitsubishi-plcs-remote-dos-attacks

Linux Kernel Privilege Escalation Vulnerability Found in RDS Over TCP

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/46iBnMY1Xmw/linux-kernel-privilege-escalation-vulnerability-found-rds-over-tcp

---

>20,000 Linksys routers leak historic record of every device ever connected

reader comments

99 with 80 posters participating

Share this story

This post has been updated to add comments Linksys made online, which says company researchers couldn’t reproduce the information disclosure exploit on routers that installed a patch released in 2014. Representatives of Belkin, the company

that acquired Linksys in 2013, didn’t respond to the request for comment that Ars sent on Monday. Ars saw the statement only after this article went live.

More than 20,000 Linksys wireless routers are regularly leaking full historic records of every device that has ever connected to them, including devices’ unique identifiers, names, and the operating systems they use. The data can be used by snoops or hackers in either targeted or opportunistic attacks.

Troy Mursch

Independent researcher Troy Mursch said the leak is the result of a flaw in almost three dozen models of Linksys routers. It took about 25 minutes for the Binary Edge search engine of Internet-connected devices to find 21,401 vulnerable devices on Friday. A scan earlier in the week found 25,617. They were leaking a total of 756,565 unique MAC addresses. Exploiting the flaw requires only a few lines of code that harvest every MAC address, device name, and operating system that has ever connected to each of them.

The flaw allows snoops or hackers to assemble disparate pieces of information that most people assume aren’t public. By

combining a historical record of devices that have connected to a public IP addresses, marketers, abusive spouses, and investigators can track the movements of people they want to track. The disclosure can also be useful to hackers. The Shadowhammer group, for instance, recently infected as many as 1 million people after hacking the software update mechanism of computer maker ASUS. The hackers then used a list of about 600 MAC addresses of specific targets that, if infected, would receive advanced stages of the malware.

Got admin?

Besides handing out device information, vulnerable routers also leak whether their default administrative passwords have been changed. The scan Mursch performed earlier this week found about 4,000 of the vulnerable devices were still using the default password. The routers, he said, have remote access enabled by default and can't be turned off as a workaround, because it's required for an accompanying Linksys App to function.

That scenario makes it easy for hackers to quickly scan for devices that can be remotely taken over. Hackers can then obtain the Wi-Fi SSID password in plaintext, change DNS settings to send connected devices to malicious addresses, or carry out a range of other compromises. A recent attack group known as the BlackTech Group likely used similar router attacks to install the Plead backdoor on targeted computers.

Mursch told Ars that his tests show that devices are vulnerable even when their firewall is turned on. He also said that devices continue to leak even after running a patch Linksys issued in 2014.

Mursch said he disclosed the information leakage publicly after he privately reported it to Linksys officials and they closed the issue after determining it "Not applicable / Won't fix." Ars emailed press representatives of Belkin, the company

that acquired Linksys in 2013, seeking comment earlier this week and never received a response.

In a statement published Tuesday, one day after Mursch's post went live, Linksys representatives wrote:

> *Linksys responded to a vulnerability submission from Bad Packets on May 7th, 2019 regarding a potential sensitive information disclosure flaw: CVE-2014-8244 (which was fixed in 2014). We quickly tested the router models flagged by Bad Packets using the latest publicly available firmware (with default settings) and have not been able to reproduce CVE-2014-8244; meaning that it is not possible for a remote attacker to retrieve sensitive information via this technique. JNAP commands are only accessible to users connected to the router's local network. We believe that the examples provided by Bad Packets are routers that are either using older versions of firmware or have manually disabled their firewalls. Customers are highly encouraged to update their routers to the latest available firmware and check their router security settings to ensure the firewall is enabled.*

As mentioned above, Mursch said the 2014 patch failed to fix the vulnerability on the routers he tested, even when the firewall was turned on. The existence of 20,000 to 25,000 actively leaking routers suggest many people have either failed to apply the patch or that the patch doesn't always work.

The list of vulnerable devices released by Mursch is here. An image is also below:

Troy Mursch
People using one of these devices would do well to test if it is leaking device history to the Internet even after installing the 2014 update. It is, users should either replace the router with a newer model or replace the Linksys firmware with a third-party offering such as OpenWrt.

https://arstechnica.com/?p=1507147

Slack Flaw Allows Hackers to Steal, Manipulate Downloads

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/1nIwS3oXunQ/slack-flaw-allows-hackers-steal-manipulate-downloads

---

Tenable Updates Free Vulnerability Assessment Solution

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/RUSBUnBAm28/tenable-updates-free-vulnerability-assessment-solution

---

Wormable Windows RDS Vulnerability Poses Serious Risk to ICS

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/buaJVps

2R44/wormable-windows-rds-vulnerability-poses-serious-risk-ics