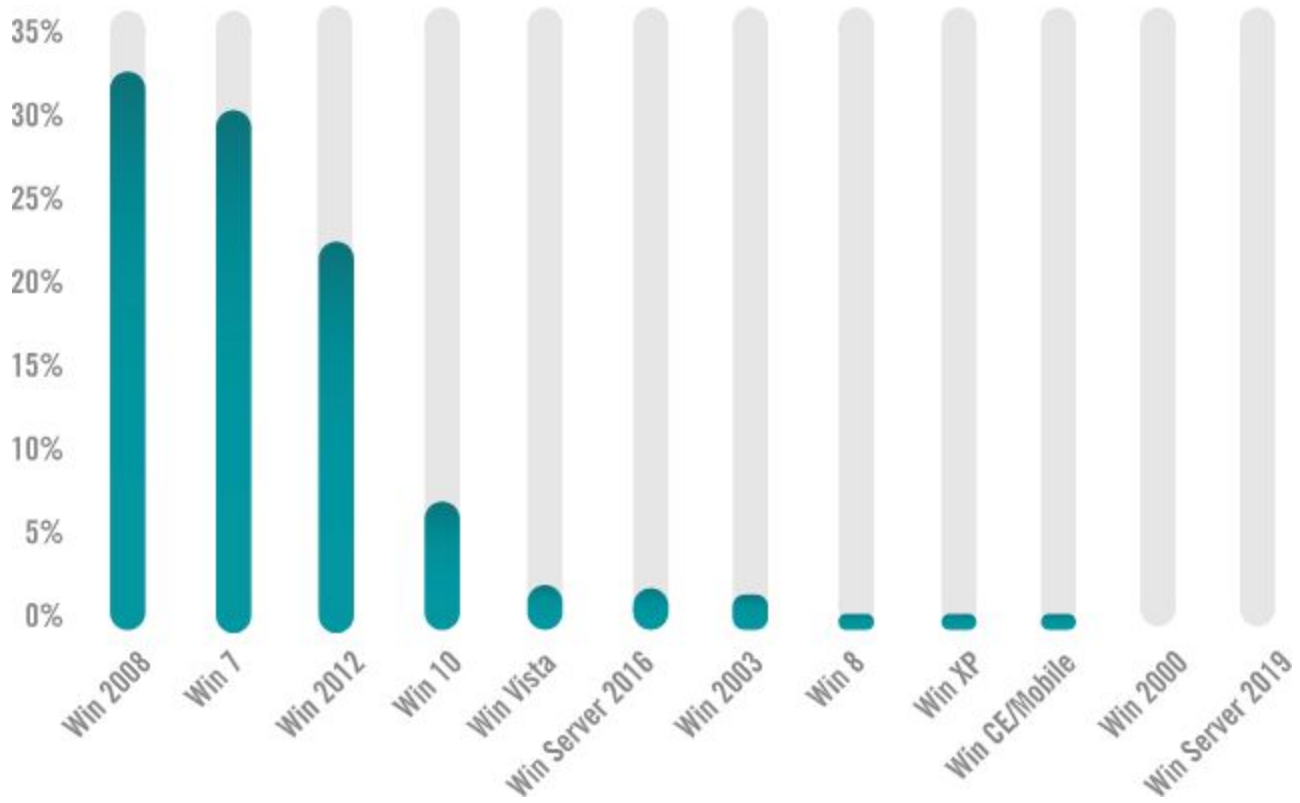
Security Now! #733 - 09-24-19

Top 25 Bug Classes

This week on Security Now!

This week we look at the driver behind this summer's comeback in cryptocurrency mining. We also check out a managed security provider's summary of the biggest problems they encounter with their more than 4000 clients. We look at the revised and worrisome update after six years of SOHO router and NAS device security, and we suggest that everyone using Chrome goto to "About/Update." I found three notes about SpinRite that I'm not sure I ever shared, so I will. Then we're conclude with the result of processing the massive CVE vulnerability database which reveals the top 25 most enduring classes of software bug impacting the security of our industry.

Windows distribution among >4000 small to mid-sized businesses:



It shows the truth of Windows 10's VASTLY lower small enterprise adoption. This means that the Win10 uptake among ***end-users*** is predictably very high -- Microsoft's force-feeding campaign was a success there; but that corporate use is lagging far far behind. This presents a dilemma for Microsoft in 2020, since their small to mid-sized business users are completely happy with Windows 7.

Security News

Cryptomining makes a comeback
We've obviously been focusing a lot recently on ransomware. But cryptocurrency mining operations are far from gone. In fact, they have been enjoying a bit of a Renaissance this summer while remaining out of the spotlight, which ransomware has claimed.

As we know, the threat landscape changed dramatically once it became possible for malefactors to turn their dastardly deeds into cold hard cash. Suddenly viruses and worms and botnets (Oh my!) were not just curios... Now they became sources of cash and recipients of much greater focus, intent, and attention.

In the case of the cryptocurrency mining world, motivation is directly tied to the cryptocurrency's exchange rate against real world currencies... and as we know, that's been quite a roller coaster ride for the past five years.

As we know, Bitcoin's "proof of work" uses a SHA256 hash with guessing to find an result having some number of least-significant bits all zero. The fact that it's SHA256 has allowed GPUs, and then ASICs, to be custom made for ultra high speed mining of Bitcoin. This has "upped the ante" for Bitcoin mining to such a level that commandeered PCs and servers don't stand a chance.

However, the Monero cryptocurrency's "proof of work" algorithm was deliberately designed to be resistant to ASIC accelerated mining, which explains why we keep hearing about Monero being the target of commandeered browsers, PCs and servers.

Monero's dollar exchange value was flying high back in 2017, in the $300 to $400 range. But it fell victim the big cryptocurrency slump through 2018, losing nearly 90% of its trading value, landing at $40 to $50 by the end of last year. But since then Monero has been steadily climbing, nearly tripling in value over this past summer and settling in around $115.

That chance in market value has not gone unnoticed, with fresh new aggressive malware campaigns ramping up to reap some ill gotten wealth.

To give everyone a sense for what's been going on, and for how ative the illicit cryptomining world has become recently, here are some snapshot events, some of which we have touched on when they broke out into the news...

- In May 2019 - An Intezer Labs report described the battle between two crypto-mining operations, the Rocke and Pascha groups, were fighting infect to same types of Linux-based cloud-based apps.

- May 2019 - A Guardicore report details a Chinese-based crypto-mining group that infected over 50,000 Windows MS-SQL and phpMyAdmin servers in the "Nansh0u campaign" to mine Monero.

- May 2019 - Trend Micro reported that the infamous RIG exploit kit had started to deploy a Monero miner as its final payload. The crypto-miner was aimed at Windows desktop users,

rather than servers, like most Monero mining operations tend to be.

- June 2019 - A Trend Micro report details a new malware strain named BlackSquid. The malware can target both Windows and Linux servers, and also uses additional exploits to move laterally through networks, to infect as many systems as possible with its crypto-mining payload.

- June 2019 - Another Trend Micro report details another malware operation whose final goal is to deploy a Monero crypto-miner. Just like BlackSquid, this malware also relied on the EternalBlue exploit to spread through internal networks after compromising an initial point of entry.

- June 2019 - And still another Trend Micro report details how the AESDDoS botnet previously focused on infecting servers to carry out DDoS attacks had shifted towards delivering a Monero miner instead. This group specifically went after Docker servers.

- June 2019 - A Sucuri report described another crypto-mining malware operation that infected web servers and used a cronjob to persist on infected hosts.

- June 2019 - A Kaspersky report describes a new malware strain named Plurox. Targeting Windows, this malware comes with several modules for performing crypto-currency mining, in various forms.

- June 2019 - ESET researchers detail LoudMiner, a malware family that targets both macOS and Windows. According to researchers, LoudMiner uses virtualization software -- QEMU on macOS and VirtualBox on Windows -- to mine Monero on a Tiny Core Linux virtual machine.

- June 2019 - Trend Micro researchers detail a Monero-mining operation during which crooks scan the internet for Android devices exposing their ADB debug ports, which they then use to plant a crypto-miner on unprotected hosts.

- July 2019 - An Intezer Labs report detailed the WatchBog cryptocurrency-mining botnet, operational since late 2018, and which compromised more than 4,500 Linux machines.

- August 2019 - A Carbon Black report [PDF] detailed changes in the activity of Smominru, one of the oldest and largest cryptocurrency mining botnets around. Besides running crypto-mining payloads, the botnet also stole credentials from infected hosts, which it later put up for sale online.

So... Though we aren't talking about cryptocurrency mining every week, it remains very much "a thing" for us to keep our eye on. And this summer’s gradual return to increased Monero mining profitability means that there will be increased pressure to steal CPU cycles wherever they can be found.

"The top three most attacked ports"
That BleepingComputer headline caught my eye, and the story led me to a recently issued 16-page report by the Managed Security Services firm "AlertLogic" titled "Critical Watch Report SMB ThreatScape 2019." It contains some interesting information and analysis that I thought our listeners would find interesting...

https://resources.alertlogic.com/c/IR-critical-watch-report

AlertLogic says that they analyzed 1.3 Petabytes of data, 10.2 Trillion log messages, 2.8 Billion Intrusion Detection System events, 8.2 Million verified incidents... all across their more than 4,000 customers. They explained and summarized as follows:

Small to mid-sized businesses (SMBs) are under greater pressure than ever to address cyber threats. Cybercriminals are increasingly targeting smaller businesses in addition to larger enterprises. The principal challenge for SMBs is that they must face these threats with fewer security resources than large enterprises. Limited budgets and staff constraints are causing many organizations to make inadequate cybersecurity investment decisions that continue to put them at risk, but forward-looking SMB leaders are seeking new ways to be 'security smart' as they address cyber risks and respond to attacks.

In providing managed security services for over 4,000 organizations, Alert Logic has first-hand insights into how small to mid-sized businesses are being attacked and the best methods for responding and reducing their attack surface. Since the publication of our last look into the cyber security threatscape in 2018, we've observed a steady increase in attacks and changes in attack methods.

Based on an analysis of the 5,000 attacks per day we detected across our customer base during the period from November 2018 to April 2019, we identified threat patterns and incorporated those into better defenses for our customers. Additionally, our security researchers actively monitored emerging and evolving vulnerabilities and attack methods across the threatscape of the open internet beyond our customer base. This research has uncovered several patterns that specifically affect small to mid-sized businesses and so we have chosen this focus for this latest Critical Watch Report on the SMB Threatscape for 2019.

Collectively, this research is based upon close examination of over 1.3 petabytes of security data, more than 2.8 billion IDS events, 8.2 million verified incidents, and the common vulnerabilities present in small to medium businesses. The results reveal nine key takeaways:

- Encryption-related misconfigurations are the largest group of SMB security issues
- In SMB AWS environments, encryption & S3 bucket configuration are a challenge
- Weak encryption is a top SMB workload configuration concern
- Most unpatched vulnerabilities in the SMB space are more than a year old
- The three most popular TCP ports account for 65% of SMB port vulnerabilities
- Unsupported Windows versions are rampant in mid-sized businesses
- Outdated Linux kernels are present in nearly half of all SMB systems
- Active unprotected FTP servers lurk in low-level SMB devices
- SMB email servers are old and vulnerable

To understand where SMBs are vulnerable and how best to address these weaknesses, Alert Logic continually scans its more than 4,000 customers to identify where they have gaps and helps organizations understand how to close those gaps. This level of partnership, part of the SIEMless Threat Management approach, is how Alert Logic supports customers and help make their security stronger every day.

In our Critical Watch Report analysis, we observed that while automated updates are having a positive impact on system patching, SMBs often struggle with misconfigurations and gaining visibility to the vulnerabilities these misconfigurations cause. For systems that remain unpatched, available patches are often more than a year old. This points again to hampered visibility, difficulty in locating vulnerabilities, and the use of legacy technology to which patches cannot be applied or are no longer provided, along with a challenge of keeping up with patching activities generally due to limited resources. SMBs also find encryption to be a challenge. Our analysis showed that 66% of workload configuration issues were related to weak encryption.

In these nine takeaways, we paint a picture of SMBs straining to keep pace with changes on the security landscape while dealing with aging infrastructure with lapsed support and limited options for security updates and bug fixes. Security has always been a challenge and these real-world observations indicate that security is particularly difficult for mid-sized businesses.

Key Takeaways

1. ENCRYPTION-RELATED MISCONFIGURATIONS ARE THE LARGEST GROUP OF SMB SECURITY ISSUES

Automated patching has made inroads in the fight to eliminate vulnerabilities in the SMB space. Patches are often distributed and can be done automatically across ecosystems. What remains as an issue is misconfigurations which can require remediations ranging from manual reviews to complete architectural redesigns. In our analysis, we determined that 13 encryption-related configuration issues account for 42% of all security issues found.

2. FOR SMB AWS ENVIRONMENTS, ENCRYPTION ISSUES AND S3 BUCKET CONFIGURATION STILL A CHALLENGE

Amazon Web Services is a strong player in the global cloud-infrastructure industry, with a market share equivalent to that of the next four public cloud providers combined.

Our analysis of AWS configuration issues shows that encryption issues affect 33 percent of the SMB instances we scanned. This indicates encryption is not yet an instinctive behavior despite being a best practice and a requirement of many regulations including PCI-DSS, HIPAA, HITECH, GBLA, GDPR, NIST, SOX, and state regulations such as CA SB 1386.In addition, while there is a significant focus on blocking inbound traffic to prevent attacks, organizations would also be well served to foil attacks by implementing basic configuration checks, preventing outbound contact to command and control servers as well as implementing measures to prevent data exfiltration. Of the SMB AWS instances we observed, more than 14 percent had significant S3 bucket configuration issues.

3. WEAK ENCRYPTION IS A TOP SMB WORKLOAD CONFIGURATION CONCERN

When we examined the top workload configuration issues, we discovered that 66 percent of the issues were related to weak encryption. Understanding and configuring encryption trade-offs within an application is difficult, and as a result, many organizations just implement the default encryption associated with an application. This presents a security challenge as many of these defaults were defined when older encryption protocols were still considered safe. As an example, OWASP shares the perspective that these encryption protocols (below) are to be avoided and yet we still see them regularly in use today:

- MD5 has recently been found less secure than previously thought. Secure applications should migrate away from this algorithm.
- SHA-0 has been conclusively broken and should no longer be used for sensitive applications.
- SHA-1 has been reduced in strength; SHA-256, which implements a larger key size, should be used instead.
- AES is the current preferred symmetric algorithm, not DES.

4. MOST UNPATCHED VULNERABILITIES IN THE SMB SPACE ARE MORE THAN A YEAR OLD

Even though automated updates have vastly improved software patching, organizations are still having difficulty keeping pace. When examining the top 20 unpatched vulnerabilities present in the SMB space, Alert Logic found that 75 percent of them are more than a year old. The use of open source software, a widespread and established technique for building software projects efficiently, can complicate the patch cycle. This is particularly true when the open source software is embedded. This is a challenge for organizations that leverage open source resources and libraries. To uncover and reduce the vulnerabilities left by this unpatched code, it is critical for all organizations to invest in third-party validation of the efficacy of the update process in the software development life cycle (SDLC). Regular vulnerability scanning is also a requirement.

5. THE THREE MOST POPULAR TCP PORTS ACCOUNT FOR 65% OF SMB PORT VULNERABILITIES

Port scanning is done regularly by both attackers and defenders. Internal security teams, blue teams, can use regular port scanning to help identify weaknesses, firewall misconfiguration issues, and to discover unusual services running on systems.

When considering their attack surface, organizations should be aware of which ports have the most vulnerabilities—which is a factor of port popularity more than a statement on the port's relative security. In examining ports, given that these ports are the ones that are exposed to the Internet it is no surprise that SSH (22/TCP), HTTPS (443/TCP) and HTTP (80/TCP) made the top three with 65 percent of the vulnerabilities. It is, however, interesting to note that the recent MS RDP BlueKeep attack targets the fourth most popular port, RDP/TCP.

As basic guidance, security across all network ports should include defense-in-depth. Ports that are not in use should be closed and organizations should install a firewall on every host as well as monitor and filter port traffic. Regular port scans and penetration testing are also best practices to help ensure there are no unchecked vulnerabilities. In addition to these steps, patch and harden any device, software, or service connected to ports to further close off avenues of attack.

Patch and harden any device, software, or service connected to the port until there are no dents in your networked assets' armor. Be proactive as new vulnerabilities appear in old and new software that attackers can reach via network ports. Lastly, be sure to change all default settings and passwords as well as running regular configuration checks.

6. UNSUPPORTED WINDOWS VERSIONS ARE RAMPANT IN MID-SIZED BUSINESSES

More than 66 percent of scanned devices are running Microsoft OS versions that will be out of support by January 2020. The current Windows Server release – 2019 – is almost undetectable while the majority of devices scanned during the period analyzed are running Windows versions that are more than 10 years old. Additionally, there are still a non-trivial number of Windows XP and even 20-year-old Windows NT devices out there. Even if they are not exposed to the internet, these targets make lateral movement relatively easy once a host has been compromised. With the discontinuation of security updates and bug fixes for Windows Server 2008 scheduled for 2020, combined with the SMB trend of holding on to old operating systems, this security issue is likely to get much worse next year.

7. OUTDATED LINUX KERNELS PRESENT IN NEARLY HALF OF ALL SMB SYSTEMS

Kernels are the heart of an operating system. They manage everything including hardware, memory, applications, and even user privileges. Kernel vulnerabilities are discovered quite frequently, and fixes are only released for supported versions. In a 2017 article, ComputerWorld described these outdated Linux kernels as the working dead

Many deployed application systems mask the underlying OS distribution flavor making it difficult to determine which kernel version is being run, however about half the systems we identified are still running a version 2.6 kernel, which has been out of support for more than 3 years. There are at least 69 known vulnerabilities for this kernel level, with many of them relatively easy to exploit and with 24 of the Common Vulnerabilities and Exposures (CVEs) scoring 7 or above on the severity scale.

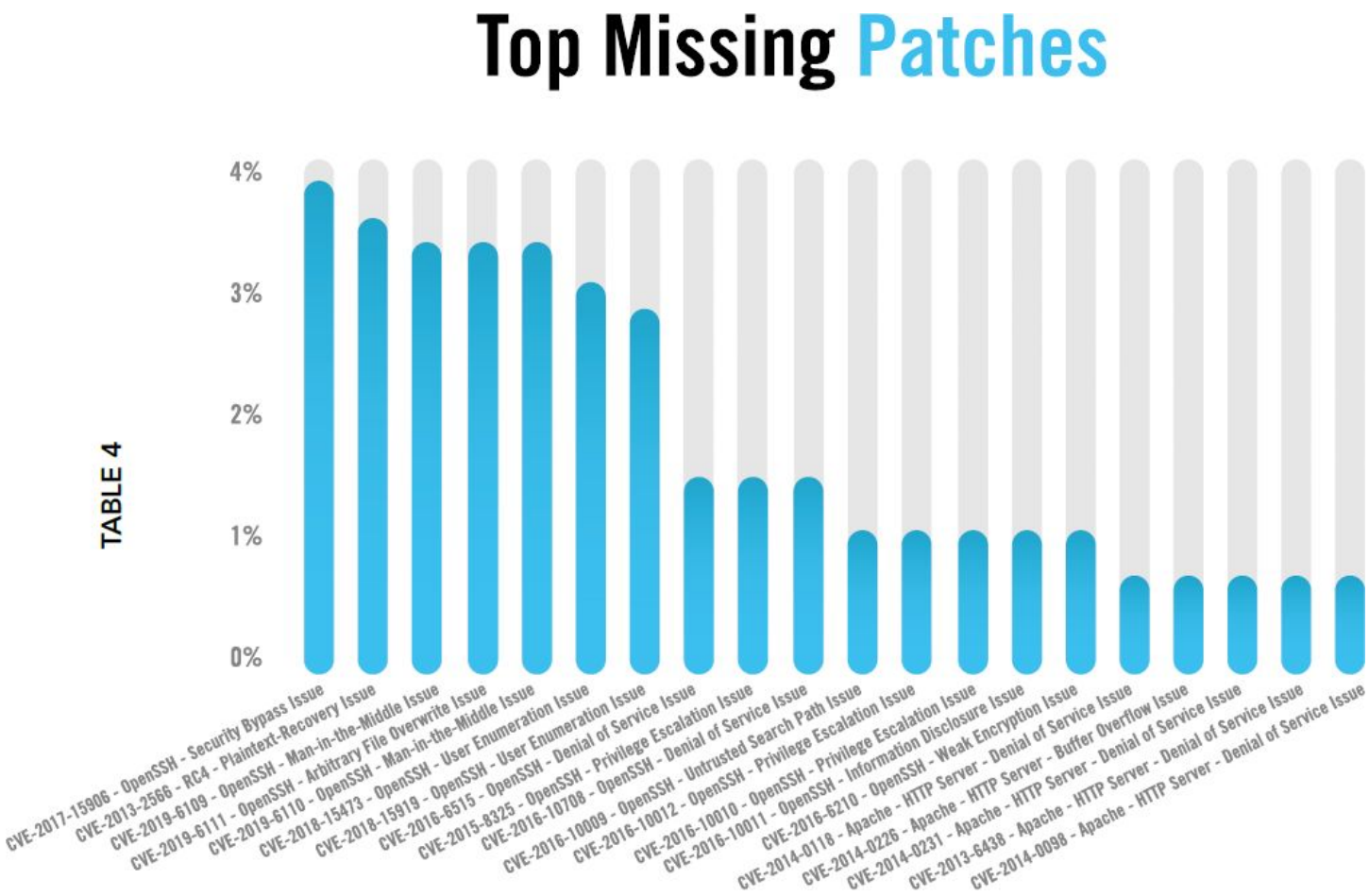
8. ACTIVE UNPROTECTED FTP SERVERS LURK IN LOW-LEVEL SMB DEVICES

The nearly 50-year-old file transfer protocol (FTP) is really showing its age from a security standpoint and yet we continue to find FTP servers in SMB environments. With a lack of built-in strong authentication and non-repudiation functionality, FTP is seriously flawed. Yet, of all the FTP servers found, very few were using SFTP for increased security. In our vulnerability scanning, we found a disturbing number of FTP servers active on printers, cameras and uninterruptable power supplies—estimated to be as much as one-third of all the FTP servers we found.

Hackers continue to use these innocent-looking devices to store and distribute malware. As a precaution, organizations should shut down unnecessary FTP servers and access, especially on devices that are not commonly monitored such as printers and power supplies.

9. SMB EMAIL SERVERS ARE OLD AND VULNERABLE

Modern businesses are fueled by email and mid-sized businesses are no exception. Without email, business communication grinds to a halt. This is why we were surprised to see that almost a third of the top email servers detected were running on Exchange 2000, which has been unsupported for almost 10 years (since July 2010). Despite being the life blood of organizations, SMBs are running the risk of email failures resulting from newly identified vulnerabilities for which patches will not be made available.



SOHOpelessly Broken...

Six years ago, back in 2013, the Baltimore, Maryland based security consultancy "Independent Security Evaluators" (ISE) tested 13 small office/home office (SOHO) routers and wireless access points. At that time they enumerated 57 security bugs and were able to take over 11 of the 13 devices from outside the local network. Their report was titled: "SOHOpelessly Broken"

We would hope that our beloved industry would have taken this to heart and enhanced its security in the last six years, right? Nope. ISE recently updated its test to "SOHOpelessly Broken 2.0."

https://www.securityevaluators.com/whitepaper/sohopelessly-broken-2/
https://www.securityevaluators.com/wp-content/uploads/2019/09/SOHO2.pdf

Once again they tested 13 devices, some from the same vendors and some new. Get this: They found more than double the number of flaws, filing 125 CVE bugs based on their research. This time around, they were able to obtain remote root access on 12 of the 13 devices.

The team tested equipment from ASUS, Buffalo, Drobo, Lenovo, Netgear, QNAP, TerraMaster, Seagate, Synology, Xiaomi, Zyxel, and Zioncom. The attacks included bypassing authentication mechanisms altogether. On one device, the team was able to hijack a cookie authentication system by changing the IP address to 127.0.0.1 and issue unauthorized requests via the authentication API.

The project found that some things had changed since 2013, and others had not. Device vendors had taken steps to try to protect their software. For example, several used address-space layout randomization (ASLR) to make memory-based attacks like buffer overflows more difficult to succesfully exploit. However, they were able to exploit other flaws to bypass ASLR and launch their buffer overflow attacks anyway.

	Buffer Overflow	Cross-Site Scripting	Command Injection	SQL injection	Authentication Bypass	Authorization Bypass	Cross-Site Request Forgery	File Upload Path Traversal
Buffalo TeraStation TS5600D1206		✓	✓		✓	✓		✓
Synology DS218j*								
ASUS RT-AC3200	✓	✓	✓					
Netgear Nighthawk R9000		✓	✓		✓	✓		
TerraMaster F2-420		✓	✓	✓	✓	✓	✓	✓
Drobo 5N2**		✓	✓		✓	✓		✓
Zyxel NSA325 v2			✓				✓	
TOTOLINK A3002RU		✓	✓		✓	✓	✓	
Asustor AS-602T		✓	✓					✓
Seagate STCR3000101		✓		✓				✓
QNAP TS-870		✓	✓				✓	✓
Mi Router 3		✓	✓					
Lenovo ix4-300d		✓	✓				✓	✓

One device encrypted the PHP files used to process requests through its web interface but, of course, it still had to store the decryption key on the device. So the ISE team used that stored decryption key to access the files and exploit those using PHP's system() function to obtain shell access.

Paraphrasing from the report:

> Perhaps more interesting are the number of features that are still missing since SOHOpelessly Broken 1.0. Features such as anti-CSRF tokens and browser security headers, which are commonplace in mainstream web applications, are still rare among our sample of devices. If vendors had implemented these basic protections we would not have been able to hack the devices.

ISE tried many types of attack, often chaining them together to successfully exploit the device. The most successful were cross-site scripting (XSS) and command injection, which are, as we know, well worn, old and well understood vulnerabilities that should also by now be well understood by firmware developers. But apparently not.

Based on their research, Synology comes out on top. Its DS218J, a device that ISE had also included in the 2013 test, did not show up in any of the broad attack categories, and it had the fewest CVEs at just two: a session fixation bug in its Photo Station application and the ability to determine metadata of arbitrary files (both medium severity). Moreover, Synology responded promptly to ISE's bug reports, which isn't something ISE was able to say about all manufacturers. Some vendors' methods for handling bug reports had improved in the last six years, and others were entirely MIA. Reporting bugs to several of the vendors was not even possible. From some of them ISE got either no co-operation or no response at all.

Six years ago, back in 2013, none of the manufacturers tested had bug bounty programs. Today, Netgear, Synology, Xaomi and QNAP all have bug bounty programs in place.

So what are our takeaways from this? ISE's reporting says that when buying a device, we should look for a history of security vulnerabilities with its vendor, along with how long the vendor takes to fix them. We should also avoid using the device with the default configuration. Turn off features that are not needed, especially all remote access features.

The report also noted that a significant number of devices are deployed and then never updated afterwards. These devices will be vulnerable to any publicly-disclosed issues, even if patched firmware is made available. So users should create some sort of tickler system to remind us to periodically check for updates from that vendor and apply them. These set-and-forget devices on our network edge are too often set and forgotten.

I'll note that MY own advice -- and I take my own advice, as I've mentioned previously -- is to use a pfSense-based firewall router out on the edge. It's running FreeBSD and pfSense. It's updated as needed and offers every possible feature -- such as OpenVPN and OpenSSH and mind-blowing NAT capabilities -- that you could ever want.

It's all 100% open source and free, and if you want to drop-in turnkey running box, the Netgate SG-1100 is a beautiful three-NIC device. SO you can easily create a truly isolated dual LAN environment with total control over what's allowed to cross where:

https://www.netgate.com/solutions/pfsense/sg-1100.html

It's $180, which is a bit steep for what it is, but the pfSense site can offer just about any alternative: https://www.pfsense.org/

They note that: "As pfSense is based on FreeBSD, its hardware compatibility list is the same as FreeBSD's. The pfSense kernel includes all FreeBSD drivers." pfSense v2.4 is based on FreeBSD v11.2. https://www.freebsd.org/releases/11.2R/hardware.html

Chrome gets an emergency update, to: 77.0.3865.90
https://chromereleases.googleblog.com/2019/09/stable-channel-update-for-desktop_18.html

Google:

> Note: Access to bug details and links may be kept restricted until a majority of users are updated with a fix. We will also retain restrictions if the bug exists in a third party library that other projects similarly depend on, but haven't yet fixed.

Google has released an urgent software update for its Chrome web browser and is urging Windows, Mac, and Linux users to upgrade the application to the latest available version immediately.

It started rolling out to users worldwide Wednesday containing security patches for 1 critical and 3 high-risk security vulnerabilities, the most severe of which could allow remote hackers to take control of an affected system.

As I noted from their statement before, Google is choosing to hold details close to their vest for the time being to prevent hackers from exploiting them and to give most users time to run Chrome and have it self-update. I'd been using Chrome all morning and it had NOT auto updated. I went to Help/About and =THEN= it updated to this latest release. So to be on the safe side, if you're using Chrome, goto Help/About and let it bring itself current if it isn't already.

All we know at the moment is that all four of the vulnerabilities are use-after-free issues in different components of the browser... with one able to cause remote code execution.

Vulnerabilities Patched By Chrome 77.0.3865.90:

- Use-after-free in UI (CVE-2019-13685) — Reported by Khalil Zhani
- Use-after-free in media (CVE-2019-13688) — Reported by Man Yue Mo of Semmle Security Research Team
- Use-after-free in media (CVE-2019-13687) — Reported by Man Yue Mo of Semmle Security Research Team
- Use-after-free in offline pages (CVE-2019-13686) — Reported by Brendon Tiszka

Google has paid out a total of $40,000 in rewards to Man Yue Mo of Semmle for both the vulnerabilities—$20,000 for CVE-2019-13687 and $20,000 for CVE-2019-13688—while the bug bounties for the remaining two vulnerabilities are yet to be decided.

Successful exploitation of these vulnerabilities only requires that a specially crafted web page be displayed. They do not require ANY user interaction.

SpinRite

Scott <...alumni.ucdavis.edu>
Location: Woodland, CA
Subject: SpinRite Guide for New Hard Drives

Hey Steve, I've heard you speak briefly about running SR on brand new drives but what metrics should we be looking at to determine if the drive is healthy or should be returned?

Jeff Gros
Location: Yorba Linda
Subject: SpinRite is too hot to handle!

Hi Steve,

I'm building a Synology 1815+. I bought six 6 TB HGST 7200 RPM drives with 128 MB cache to run in SHR2 (essentially RAID 6) and a 240 GB Kingston HyperX Savage SSD for the Synology to use as a cache.

As usual, I run SpinRite level 4 on all spinning drives and level 1 on the SSD before putting them to use.

My resident SpinRite machine is 2000's era machine which now runs Linux. However, because this machine is a tower and the SATA cables are near the top, I have to make my own tower out of books and boxes to get the drive to reach the cables.

I made the tower out of some boxes with some computer paper towards the top. However, I was worried about the computer paper getting hot and starting a fire. I had some anti-static bubble wrap, so I put this directly under the drive. If it does get too hot it will just melt the plastic. What could go wrong? Perfectly safe...

Well, you can probably see where this is going. When I came back to check on the drive a few hours later, SpinRite greeted me with a RED SCREEN OF DEATH! SpinRite halted because the drive was too hot! The screen showed 133 F (not sure if SpinRite dynamically updates this screen or if it was the last reading before halting). I immedidately turned off the machine and detatched the drive. Boy was it hot to the touch! I cooled it as much as possible with some compressed air and let it sit.

Now I know why you have heatsinks on your harddrives in that new machine you built. Drives need to breathe!

The next day I tried again, but gave more thought to my tower (no flammables and no plastic). I also added a desk fan that I use during soldering (net effect was about 10 F with the fan on full blast according to SpinRite). The drive seemed to have no memory of going to hell and back.

Steve, thanks for saving my $250 drive from the stupidity of this now humbled SpinRite user. With your help, I now have the Synology up and running!

Also, thanks for your recent tip of afraid.org and the Hover CNAME for DDNS. I'll be trying that out soon enough!

Thanks

Jeff

John Fletcher
Location: Nottingham, England
Subject: SSHD Drive

Having just installed a new Samsung 1Tb SSDH with 32Gb Nand cache (ST1000LX001) my thoughts turned to what Spinrite would actually be testing on level 4, the memory or the platters?

I have been listening to Security Now since the 1st episode. The first 149 episodes I listened to in hospital in one hit as I had to remain awake for 24 hours after eye surgery and stay in for a few more days.

The Top 25 Bug Classes

2019 CWE Top 25 Most Dangerous Software Errors

We're all familiar with the "CVE" - Common Vulnerabilities and Exposures (CVE) - we talk about CVE designations every week. But there's also a CWE, the "Common Weakness Enumeration" https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html

Introduction
The Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Errors (CWE Top 25) is a demonstrative list of the most widespread and critical weaknesses that can lead to serious vulnerabilities in software. These weaknesses are often easy to find and exploit. They are dangerous because they will frequently allow adversaries to completely take over execution of software, steal data, or prevent the software from working. The CWE Top 25 is a community resource that can be used by software developers, software testers, software customers, software project managers, security researchers, and educators to provide insight into some of the most prevalent security threats in the software industry.

To create the list, the CWE Team used a data-driven approach that leverages published Common Vulnerabilities and Exposures (CVE®) data and related CWE mappings found within the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD), as well as the Common Vulnerability Scoring System (CVSS) scores associated with each of the CVEs. A scoring formula was then applied to determine the level of prevalence and danger each weakness presents. This data-driven approach can be used as a repeatable, scripted process to generate a CWE Top 25 list on a regular basis with minimal effort.

Rank	ID	Name	Score
1	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	75.56
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.69
3	CWE-20	Improper Input Validation	43.61
4	CWE-200	Information Exposure	32.12
5	CWE-125	Out-of-bounds Read	26.53
6	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24.54
7	CWE-416	Use After Free	17.94
8	CWE-190	Integer Overflow or Wraparound	17.35
9	CWE-352	Cross-Site Request Forgery (CSRF)	15.54
10	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path	14.10

		Traversal')	
11	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11.47
12	CWE-787	Out-of-bounds Write	11.08
13	CWE-287	Improper Authentication	10.78
14	CWE-476	NULL Pointer Dereference	9.74
15	CWE-732	Incorrect Permission Assignment for Critical Resource	6.33
16	CWE-434	Unrestricted Upload of File with Dangerous Type	5.50
17	CWE-611	Improper Restriction of XML External Entity Reference	5.48
18	CWE-94	Improper Control of Generation of Code ('Code Injection')	5.36
19	CWE-798	Use of Hard-coded Credentials	5.12
20	CWE-400	Uncontrolled Resource Consumption	5.04
21	CWE-772	Missing Release of Resource after Effective Lifetime	5.04
22	CWE-426	Untrusted Search Path	4.40
23	CWE-502	Deserialization of Untrusted Data	4.30
24	CWE-269	Improper Privilege Management	4.23
25	CWE-295	Improper Certificate Validation	4.06

Weaknesses On the Cusp

As in years past, the CWE team feels it is important to share additional CWEs that scored just outside of the top 25. Per the 2019 scoring formula against the NVD dataset, these weaknesses were potentially not severe enough, or not prevalent enough, to be included in the 2019 list.

Developers that complete mitigation and risk decision-making on the 2019 CWE Top 25 may want to look for these other weaknesses potentially present in their software. For these reasons, users of the 2019 CWE Top 25 should seriously consider including these additional weaknesses in their analyses:

Rank	ID	Name	Score
[26]	CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')	3.53
[27]	CWE-522	Insufficiently Protected Credentials	3.39
[28]	CWE-704	Incorrect Type Conversion or Cast	3.25
[29]	CWE-362	Concurrent Execution using Shared Resource with Improper	3.11

		Synchronization ('Race Condition')	
[30]	CWE-918	Server-Side Request Forgery (SSRF)	2.65
[31]	CWE-415	Double Free	2.32
[32]	CWE-601	URL Redirection to Untrusted Site ('Open Redirect')	2.31
[33]	CWE-863	Incorrect Authorization	2.00
[34]	CWE-862	Missing Authorization	1.76
[35]	CWE-532	Inclusion of Sensitive Information in Log Files	1.59
[36]	CWE-306	Missing Authentication for Critical Function	1.50
[37]	CWE-384	Session Fixation	1.34
[38]	CWE-326	Inadequate Encryption Strength	1.34
[39]	CWE-770	Allocation of Resources Without Limits or Throttling	1.27
[40]	CWE-617	Reachable Assertion	1.23