Digital Security
Progress. Protected.

Remote Desktop Protocol:
Configuring remote access for a secure workforce

Using Remote Desktop Protocol (RDP) to manage your network through a crisis? Make sure you are limiting your risk by leveraging good practices, authentication tools, and the existing knowledge base.

The COVID-19 pandemic pushed enterprises around the world to send their people home and leverage any tools possible to continue operations remotely. This included RDP technology which has since seen increasing abuse. Numerous instances have emerged of attackers finding ways to exploit poorly configured settings or weak passwords to gain access to company networks.

Once inside, attackers have an open door to do almost anything, including the theft of intellectual property or other sensitive information and encrypting it for ransom.

Author: Aryeh Goretsky
Contributor: Rene Holt

July 2022

AUTHOR'S NOTE:

This is a revised edition of ESET's white paper ***RDP: Configuring Security For A Remote, But Not Distant Future,*** and was updated approximately two years after initial publication, which took place near the start of the global COVID-19 pandemic in April 2020. Since then, business has changed dramatically, with work from home becoming the new norm in many industries and offices, including many for whom work has always been performed on-premises.

This shift to a remote workforce has meant the deployment of many technologies rapidly and in quantities that would have been unimaginable pre-pandemic. Laptop computers, VPNs, and two-factor authentication are among the technologies that have been widely deployed, oftentimes correctly but sometimes not, leading to breaches, theft, and the destruction of data. One technology that has seen an uptick in use is RDP, which allows desktops and servers at the office to be accessed from home.

Even when a technology like RDP is deployed correctly, unpatched vulnerabilities can make it insecure when it is internet-facing.

In this revised paper, the author will update us on how attacks progressed throughout 2020 and 2021 using RDP.

01

What do attackers do with RDP?

In the past few years, ESET has seen a rising number of incidents in which attackers connected to Windows servers over the internet using RDP and logged on as administrators. This implies various attack vectors, including vulnerabilities such as BlueKeep, phishing, credential stuffing, password spraying, brute-force attacks, and poorly configured access to internal systems.

Once attackers are logged into a server as an administrator, they will typically perform some reconnaissance to determine what the server is used for, by whom, and when it is being used. Then they typically perform additional malicious actions like the following:

- clearing log files containing evidence of their presence on the system
- disabling scheduled backups and shadow copies
- disabling security software or setting up exclusions in it (which is allowed for administrators)
- downloading and installing various programs onto the server
- erasing or overwriting old backups, if they are accessible
- exfiltrating data from the server
- securely overwriting and deleting business-critical data

This is not a complete list of all they can do, nor are they necessarily going to perform all of these activities. While the exact frequency, sequence, and nature of what attackers will do varies greatly, four of the most common are:

- installing coin-mining programs in order to generate cryptocurrency, such as Monero
- installing ransomware in order to extort money from the organization, often to be paid using cryptocurrency, such as Bitcoin
- downloading confidential files and threatening to share them unless an extortion is paid
- in some cases, attackers might install additional remote-control software to maintain access (persistence) to compromised servers in case their RDP activities are discovered and terminated

Notable malicious RDP activity

One prolific ransomware, GandCrab, which operated until May 2019, used a Ransomware-as-a-Service (RaaS) business model in which the developers contracted affiliates to further distribute the malware. GandCrab targeted managed service providers (MSPs), making the initial breach via exposed RDP endpoints and then commandeering the MSP's remote management tools to deploy ransomware and extort multiple customers at once.

After GandCrab's operators announced their retirement some saw the rise of Sodinokibi at about the same time as the new face of GandCrab with the same actors at work. Although there are some similarities between the source code of GandCrab and Sodinokibi, our experts think that the differences indicate rather that GandCrab's source code may have been sold to a different group that developed it further to become Sodinokibi. Sodinokibi ransomware appeared just as GandCrab started to suspend its operations, essentially replacing GandCrab and using similar tactics, techniques and procedures as its predecessor to target MSPs via RDP.

The MSP connection is notable for enterprises too, as MSPs hold the keys to the kingdom for thousands of SMBs (including their business relationships), and even some enterprises. On the MSP client side, businesses face similar dependencies as both teams and individual users depend on admins for help with everything from licensing and updates to security.

RDP vulnerabilities open a big door to risk

Attacks via RDP have been slowly, but steadily, increasing and become the subject of a number of governmental advisories from the FBI, the UK's NCSC, Canada's CCCS, and Australia's ACSC, to name a few.

In May 2019, the floodgates opened with the arrival of CVE-2019-0708, aka BlueKeep, a security vulnerability in Remote Desktop Services affecting:

- WINDOWS 2000
- WINDOWS XP
- WINDOWS VISTA
- WINDOWS 7
- WINDOWS SERVER 2003
- WINDOWS SERVER 2003 R2
- WINDOWS SERVER 2008
- WINDOWS SERVER 2008 R2

01

Windows 8 and Windows Server 2012 and later were unaffected by BlueKeep, but in August, 2019, two additional wormable vulnerabilities in Remote Desktop Services allowing remote code execution via RDP were identified affecting:

- Windows 7
- Windows 8.1
- Windows 10
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Microsoft Remote Desktop for Mac
- Microsoft Remote Desktop for iOS
- Microsoft Remote Desktop for Android

Known individually as CVE-2019-1181 and CVE-2019-1182 by Microsoft, these vulnerabilities have been referred to as DejaBlue because of their similar nature. Unlike BlueKeep, DejaBlue was discovered internally by Microsoft, so there were no known instances of it being exploited in the wild prior to discovery.
While some of these are legacy systems, and in most cases are either no longer supported or only have limited vendor support, telemetry from 2019–2020 suggests there were many vulnerable systems still in use.

The BlueKeep and DejaBlue vulnerabilities allow attackers to run arbitrary program code on their victims' computers. While attackers already pose a formidable threat with automated tools at hand to speed up attacks, these vulnerabilities are wormable, which means that an attack could spread itself automatically across networks without any intervention by users, just as the Win32/Diskcoder.C (aka NotPetya) and Conficker worms have in the past.

ESET offers a free BlueKeep (CVE-2019-0708) detection tool to help identify systems vulnerable to exploitation via RDP. For instructions on its use and to download a copy, see this article.

The exploitation of wormable vulnerabilities is generally considered a severe issue. BlueKeep and DejaBlue scored the highest severity level[1] of "critical" reaching a 9.8 in the Common Vulnerability Scoring System (CVSS).

Microsoft credited NCSC for reporting the BlueKeep vulnerability and issued a blogpost strongly recommending users to install the patches, even for out-of-support operating systems such as Windows XP and Windows Server 2003. Concerns about a wormable exploit were so high at the time that, in June 2019, the US National Security Agency issued a rare advisory recommending installation of Microsoft's patches for the flaw.

[1] As a CNA, Microsoft defined the vector string and from that a score and severity level was automatically derived.

Although DejaBlue had the same level of severity as BlueKeep, DejaBlue did not trigger the same level of attention because it was likely not known to third parties prior to Microsoft's disclosure.

No major escalations in BlueKeep activity were reported until November 2019 when a hacker group was seen attempting to deploy a BlueKeep exploit at scale. These attacks had limited success, with about 91% of vulnerable computers crashing with a stop error (aka a bug check or Blue Screen of Death). However, on the remaining 9% of vulnerable computers, these attackers successfully installed Monero cryptomining software. While not the feared wormable attack, the criminal group automated exploitation, albeit without a high success rate.

The good news, in as much as such that can be said about a vulnerability like BlueKeep, is that ESET has steadily seen a decrease in detections of attacks attempting to exploit this vulnerability, from a height of over 651,000 attacks in the second quarter of 2020 to just over 365,000 in the fourth quarter of 2021, a decrease of about 44%. While there are likely several underlying causes for this decrease in exploitation attempts using BlueKeep, such as the patching of affected operating systems and the deployment of security tools at the network perimeter, it should be kept in mind that RDP attacks are still on the rise, as noted in the next section below.

Figure 1. CVE-2019-0708 "BlueKeep" detections worldwide *(source: ESET telemetry)*

As this is not one of ESET's threat intelligence reports, we will not be providing detailed technical descriptions of these vulnerabilities and instead focus on what should be done to protect networks against this threat.

Beyond BlueKeep, RDP attacks continue unabated

While we have seen a decrease in BlueKeep attacks, we have not seen a similar trend in RDP attacks overall, and RDP continues to be a prime target for attackers seeking ingress to networks for reasons ranging from corporate espionage to ransomware and perhaps even nation-state actions.

Using malicious software and attacking networks for financial gain are nothing new. Adware and potentially unwanted software has been a problem for over twenty years, as has seizing computing resources to perform distributed denial-of-service (DDoS) attacks, but the rise of ransomware and theft of corporate secrets (often with subsequent extortion) has massively increased attempted network intrusions using RDP.

Whether it's brute-force or password spraying attacks, or other forms of attempting to gain access via RDP, the increase in the number of malicious connection attempts is mind-boggling. To give some idea of how the scale of attempted malicious RDP connections has increased, in the first quarter of 2020, ESET detected approximately 1.97 billion attempted connections. Just two years later, in the fourth quarter of 2021, about 166.37 billion connection attempts were made, which is an increase of over 8,400%.

The sheer volume of increase in these attacks indicates they must be highly automated, while the number indicates that attackers can derive tremendous value from compromising a network.

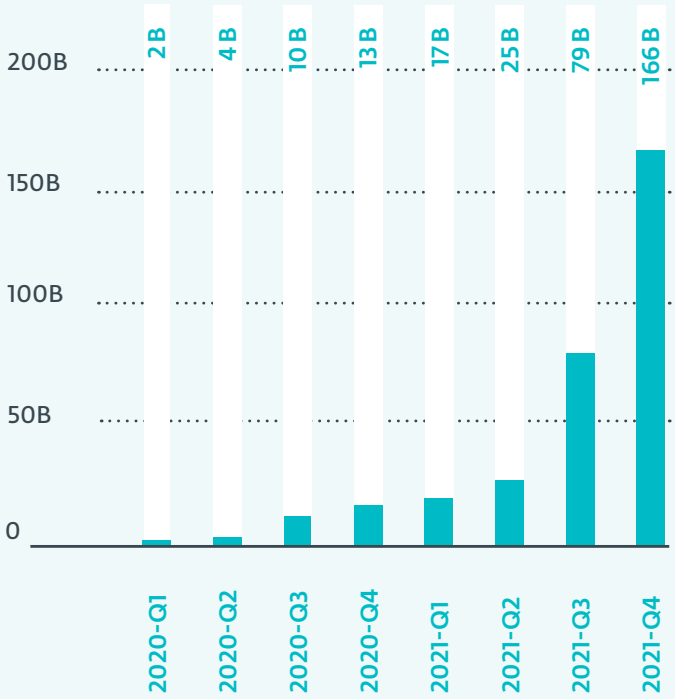

Figure 2. Malicious RDP connection attempts detected worldwide *(source: ESET telemetry)*. Absolute numbers are rounded

02

Defending against RDP-borne attackers

So, what can you do? Well, the first thing, is to stop connecting directly to your servers over the internet using RDP or at least minimize this whenever possible. This may be problematic for many businesses, especially now that many employees may still be working remotely and perhaps anticipate remaining in that state in the foreseeable future.

Let us stress, if you are still running unsupported operating systems like Windows Server 2008 or Windows 7 (which are no longer supported as of January 2020), or do not have a strong patching regimen for Windows 8.1, Windows 10, or their comparable Windows Server versions, yet have machines running these platforms that are directly accessible via RDP, then you are at risk of attack and you should take remediation steps immediately. By running these platforms, your threat surface has multiplied by a substantial factor, and **the recommendations below should take a back seat to your business updating to platforms that are fully supported by their respective vendors.**

For those running up-to-date platforms, the situation does not mean that you have to immediately stop using RDP, but that you need to take additional steps to secure it as soon and as thoroughly as possible. To this end, we have created a table with the **top 15 steps you can take now to begin securing your computers from RDP-based attacks.**

	RECOMMENDATION FOR SECURING RDP	REASON
1	Disallow external connections to local machines on port 3389 (TCP/UDP) at the perimeter firewall*	Blocks RDP access from the internet altogether.
2	Test and deploy patches for the CVE-2019-0708 (BlueKeep) vulnerability and enable Network Level Authentication as quickly as possible.	Installing Microsoft's patch and following their prescriptive guidelines helps ensure devices are protected against the BlueKeep vulnerability.

3	For all accounts that can be logged into via RDP, require complex passwords (a long passphrase containing 15+ characters with no phrases related to the business, product names, or users is mandatory).	Protects against password-guessing and credential-stuffing attacks. It is incredibly easy to automate these and increasing password length makes them exponentially more resistant to attacks.
4	For accessing servers, use unique passwords for local accounts with admin rights (e.g., by using LAPS or a robust password manager service) **Also:* *Restrict server access rights to a limited group of users.*	In addition to the aforementioned reason, it also reduces the attack surface of servers by limiting the users who can access them.
5	Enable account lockout policies in Windows to prevent password-guessing attempts.	Prevents manual attacks such as credential stuffing, password-guessing, and password sprays that fall below brute force detection thresholds. Enabling account lockout policies is now the default in Windows 11, but can also be enabled in Windows 10.
6	Set the RDP client connection's encryption level to "high", if possible. If not, use the highest encryption level available for connections.	Use 128-bit encryption for all client-server communications, if possible.
7	Install a multi-factor authentication (MFA) solution, such as ESET Secure Authentication, and require it for all accounts that can be logged into via RDP, as well as for all administrator accounts.	Requires a second layer of authentication only available to employees via mobile phone, token, or other mechanism for logging into computers.
8	Install a virtual private network (VPN) gateway to broker all RDP connections from outside your local network.	Prevents RDP connections between the internet and your local network. Allows you to enforce stronger identification and authentication requirements for remote access to computers.
9	Ensure that your endpoint security software settings are locked with a strong password unrelated to administrative and service accounts.	Prevents unauthorized disabling of endpoint protection should an attacker gain administrator access in your network.
10	Enable the detection of potentially unsafe applications in your endpoint security software.	This blocks unsafe applications, including those that can terminate processes, especially those of your security products.

11	Make sure brute-force attack protection is enabled in your endpoint security software.	This detects external IP addresses that indicate an incoming brute-force attack on RDP or SMB services.
12	Enable exploitation blocking in endpoint security software, which is a non-signature-based anomaly detection technology that monitors the behavior of commonly targeted applications.	Many endpoint security programs can also block exploitation techniques. Verify that this functionality is enabled.
13	Isolate any insecure computer that needs to be accessed from the internet using RDP.	Implement network isolation to block vulnerable computer(s) from the rest of the network.
14	Replace insecure computers.	If a computer cannot be patched against the BlueKeep vulnerability, plan for its timely replacement.
15	Consider instituting GeoIP blocking at the VPN gateway.	If staff and vendors are in the same country, or a short list of countries, consider blocking access from other countries in order to prevent connections from foreign attackers.

This table is loosely based on order of importance and ease of implementation, but that can vary depending upon your organization. Some may not be applicable or may be more practical to do in a different order. Your organization may need to fine-tune these or take additional steps.

*By default, RDP operates on port 3389. If you have changed this port to a different value then that is the port that should be blocked.

NOTE: While changing the default port used by RDP can stop simple reconnaissance from low-skilled adversaries, it is widely known that many organizations simply change the default port. The ability to detect RDP traffic on non-standard ports is a well understood concept.[2,3] Port scanning services like Shodan even recommend not searching by port anymore, due to protocols like RDP being commonly used on non-standard ports.[4]

[2] Snort Rule Sid 1-49040. Available via: <https://www.snort.org/rule_docs/1-49040>

[3] Wireshark Wiki: RDP. Available via: <https://wiki.wireshark.org/RDP>

[4] Matherly, John. Don't Search by Port. Available via: <https://blog.shodan.io/dont-search-by-port/>

03

How ESET helps protect your RDP

Some good first steps are making sure that your endpoint security software is A. up-to-date, and B. detects BlueKeep exploits. BlueKeep exploits are detected as RDP/Exploit.CVE-2019-0708 by ESET's Network Attack Protection module, which is an extension of ESET's firewall technology present in ESET's endpoint protection products version 7 and higher.

Another layer of technology critical to protecting RDP is Exploit Blocker, which monitors typically exploitable applications, such as browsers, document readers, email clients, legacy Flash apps, Java, and more. Instead of aiming only at particular CVE identifiers, it focuses on exploitation techniques. When triggered, the threat is blocked immediately on the machine.

In addition to using multi-layered protection, we would advise you to put security processes in place that are as user-friendly as possible supported by easy-to-use tools. Since securing RDP requires several (procedural) steps, the use of multi-factor authentication (MFA) is perhaps most crucial because it acts as a protection against weak or brute-forced passwords. By focusing on authentication to a system or platform, in this case RDP, you protect one of the most critical systems you have in your business for managing the security of both your network and individual users.

Our MFA solution, ESET Secure Authentication (ESA), protects RDP logins by adding multi-factor authentication.

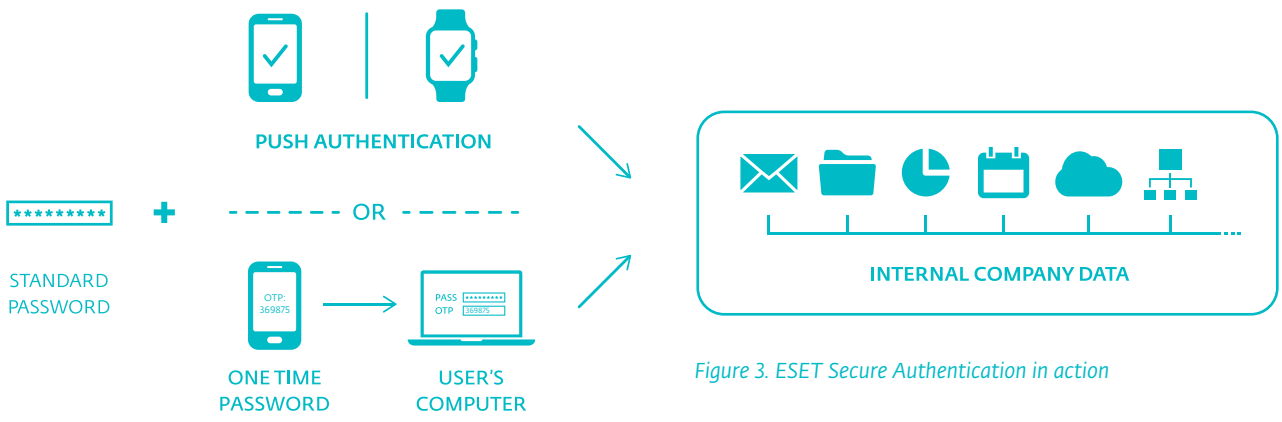

Figure 3. ESET Secure Authentication in action

ESA also supports VPNs (itself a critical safeguard securing access), Windows logins (critical for devices that contain sensitive data), cloud services such as Microsoft 365, Google Apps, and Dropbox, and many other identity and service providers.

Centrally managed from the browser, ESA works with all iPhone and Android mobile devices, and offers multiple authentication options, including easy-to-use push notifications, mobile applications, hardware tokens, FIDO security keys, and other custom methods (via the ESA Software Development Kit). Ultimately, ESA helps secure company data and cloud assets in a simple, yet powerful, way and helps businesses meet compliance requirements for regulations such as GDPR.

Lastly, adding full disk encryption as a follow-up to MFA is a great step too. ESET Full Disk Encryption provides powerful encryption of system and non-system disks that is protected by pre-boot authentication. The solution is managed natively via the ESET PROTECT management console, further improving your organization's control over data security.

Knowledge is power... full security too

Various RDP techniques and tactics can also be examined in the MITRE ATT&CK® knowledge base. While referenced by many vendors' researchers, ATT&CK brings much of this to a shared space. Leveraging ATT&CK and extended detection and response (XDR) tools together can be very useful for examining in detail threats facing your network. Tools like ESET Inspect allow security admins to examine detections, which reference ATT&CK for further information, and set custom rules tailored to each network.

A danger with RDP-borne threats is having a limited opportunity to distinguish between legitimate and malicious account use. After all, once RDP credentials have been compromised, any subsequent actions are performed in the name of a legitimate account within your organization. XDR can play a critical role in such scenarios where there is likely a need to link together several suspicious activities to identify the intrusion.

Another example demonstrating the power of XDR can be seen by considering a BlueKeep exploit that in some cases immediately crashed the targeted system because it proved unreliable. In order for this exploit to have worked, it may have needed to be paired with another exploit for an information disclosure vulnerability (for example, one of the many Adobe Flash vulnerabilities) that would reveal exploitable memory addresses. This could reduce the likelihood of a crash and thus the exploit's success rate as it otherwise frequently guessed invalid addresses.

These types of malicious behaviors can be flagged with custom rules created within ESET

Inspect, the XDR-enabling component of the ESET PROTECT platform, ultimately triggering an alarm and drawing the admin's attention. Additional network intelligence may also be sourced via regular penetration testing, and checking suspicious behavior via a security information and event management (SIEM) tool or an intrusion detection service (IDS).

CONCLUSION

COVID-19 has changed the way organizations work, not just temporarily throughout the course of the pandemic, but forever. Employers need to adjust not just to the demands of employees working from home now, but in the future as well.

One thing the pandemic has shown us is that many jobs and tasks that formerly were thought of as requiring employees to be at the office will now be viewed as optimal candidates for remote work. But, in order for that to occur, remote workers need to have secure access to the corporate network. ESET offers a variety of solutions that can help businesses provide secure access to corporate resources.

MORE TO KNOW ABOUT SMB ATTACKS

Although not directly related to RDP, Server Message Block (SMB) is another network communications protocol from Microsoft. Originally developed in the early 1990s for Windows NT, SMB allows the sharing of files and printers across networks. Because of this, it can be thought of as a "companion" protocol to RDP. And, like RDP, it is subject to wormable attacks.

In March 2017, CVE-2017-0144, also known as EternalBlue, was leaked. Reportedly developed by the US National Security Agency, it was allegedly used covertly for several years before its theft within a tranche of documents stolen from the agency. EternalBlue affected just SMB version 1 (SMBv1), the original standard for the protocol. SMB version 2 (SMBv2), released in 2006, and later versions were unaffected, but SMBv1 was still widely in use.

Microsoft promptly released a security update for the vulnerability in March 2017, but two months later in May 2017, there were still many unpatched and unprotected systems, and these were affected by the WannaCryptor (also known as WannaCry and WannaCrypt) wormable ransomware. Even in 2018 and 2019 (one and two years later, respectively), ESET was still seeing a rise in attacks exploiting this vulnerability

Sometimes, though, ESET gets to be the bearer of good news. After peaking in the third quarter of 2020 with nearly 15.4 million attempted attacks, ESET saw a decline in 2021 of attempts to exploit CVE-2017-0144, with just over 6.1 million attempted attacks, a decline of just over 60%.

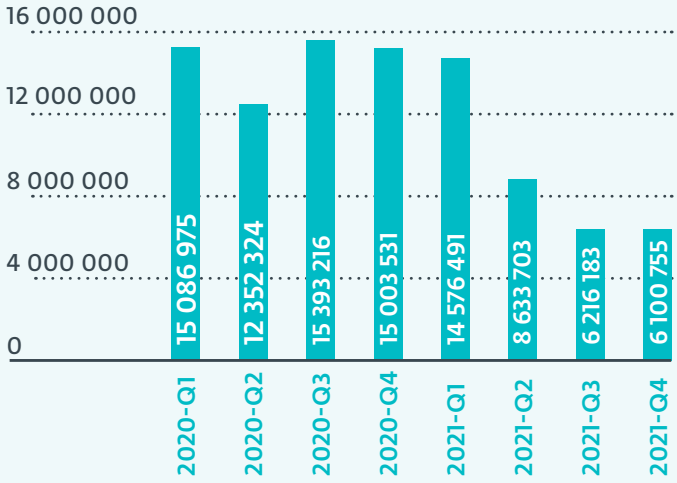

Figure 4. *CVE -2017-0144 "EternalBlue" detections worldwide (Source: ESET telemetry)*

As with CVE-2019-0708 (BlueKeep), there are likely to be several underlying causes for this decrease in exploitation attempts; however, the three most likely reasons are the rapid deprecation of SMBv1 to newer, more secure versions of the protocol; the patching of affected operating systems; and the deployment of security tools throughout the network.

Despite its age, SMBv1 may still be used in any networks in order to support older versions of Microsoft Windows, or devices such as network printers, scanners, multifunction devices, network-attached storage (NAS) devices, industrial and laboratory equipment, and so forth.

Tips for securing SMB

To this end, we have created a table with the **top seven steps you can take to begin securing your computers from SMB-based exploits.**

	RECOMMENDATION FOR SECURING RDP	REASON
1	Disallow external connections to local machines on port 445 (TCP/UDP) at the perimeter firewall.	Blocks SMB access from the internet altogether.
2	Identify which computers and devices on your network still use SMBv1. Update them to only use SMBv2/SMBv3.	Identify and remediate vulnerable systems.
3	If the device(s) cannot be replaced, isolate from the internet as well as all internal computers except those requiring access.	Implement network isolation to block vulnerable computer(s) from the rest of the network.
4	Replace insecure computers.	If a computer cannot be patched against the EternalBlue vulnerability, plan for its timely replacement.
5	Segment the network so that SMB traffic is not allowed globally; limit SMB traffic to those subnets requiring it.	Prevents or delays network penetration, slows or prevents spread of worms that propagate via SMB.
6	Make sure brute-force attack protection is enabled in your endpoint security software.	This detects external IP addresses that indicate an incoming brute-force attack on RDP or SMB services.
7	Enable exploitation blocking in endpoint security software, which is a non-signature-based anomaly detection technology that monitors the behavior of commonly-targeted applications.	Prevents RDP connections between the internet and your local network. Allows you to enforce stronger identification and authentication requirements for remote access to computers.

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide. ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

ESET IN NUMBERS

1bn+
internet users protected

400k+
business customers

200+
countries & territories

13
global R&D centers

SOME OF OUR CUSTOMERS

MITSUBISHI MOTORS
Drive your Ambition

protected by ESET since 2017 more than 9,000 endpoints

Allianz Suisse

protected by ESET since 2016 more than 4,000 mailboxes

Canon
Canon Marketing Japan Group

protected by ESET since 2016 more than 32,000 endpoints

T

ISP security partner since 2008 2 million customer base

eset®

Digital Security
Progress. Protected.