

The CalCom Software Guide to RDP Hardening

Practical Steps to Strengthen Remote Desktop
Protocol Security

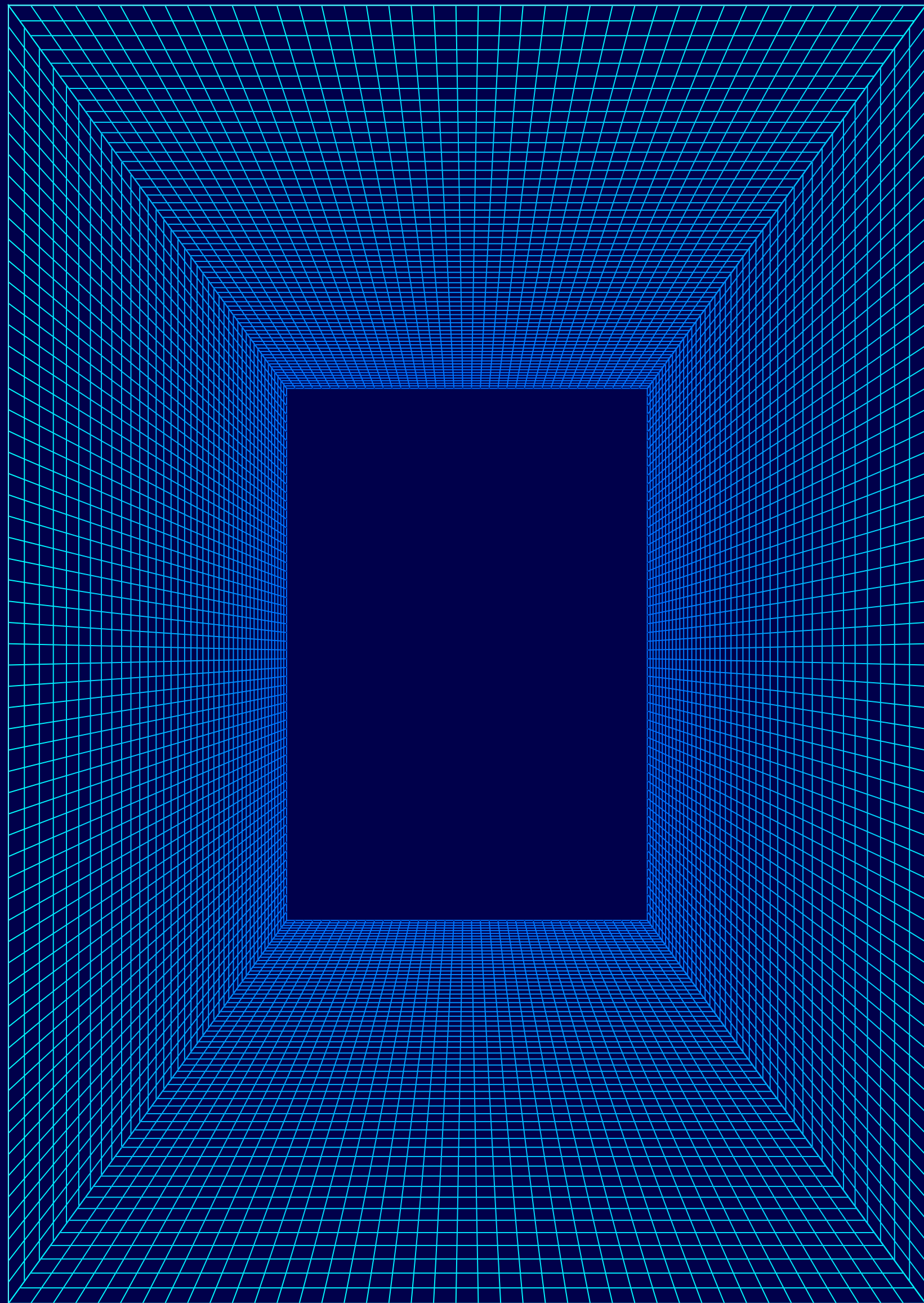
Executive Summary

Microsoft's [Remote Desktop Protocol \(RDP\)](#) is an essential tool for accessing and managing remote Windows systems. However, RDP's ubiquity and ease of use make it an attractive target for [hackers](#).

This guide breaks down what makes RDP vulnerable, how attackers are exploiting it today, and what you can do to harden your systems using the [CIS Windows Server Security 2025 Benchmarks](#). It also explains how [CalCom](#) automates RDP server hardening and share an extensive list of resources if you want to learn more.

Note

This guide focuses on RDP security. For more information on RCS security, see [CalCom's RCS Hardening Guide](#). The differences between RDP and RCS are explained below.



What You Will Learn

- What makes RDP a prime target for hackers
- Why you need to improve your organization's RDP security
- How recent attacks exploited bad RDP configuration
- The three areas of RDP security you need to improve now
- Practical advice to harden your RDP deployments
- Industry standard recommendations based on trusted sources
- How CalCom CHS helps you automate RDP protection

What is Remote Desktop Protocol, and What Makes It Vulnerable

Microsoft's [Remote Desktop Protocol \(RDP\)](#) is a key component of Microsoft's [Remote Desktop Services \(RDS\)](#). RDS is the software that manages remote access to a Windows while RDP is the protocol used to communicate between the server and client. RDP is based on the T.120 series of protocols and is compatible with multiple network topologies, including [TCP/IP](#) and [UDP](#). You connect to RDP through port 3389. The protocol can support up to 64,000 data channels. RDS and RDP were initially released as Windows NT 4.0 Terminal Server, back in 1998. From Windows Server 2008 R2, Service Pack 1, the platform was renamed to Remote Desktop and included in each subsequent release.

RDP's convenience, familiarity, and popularity also make it an ideal method for hacking Windows-based infrastructure. RDP provides an entry point for attackers to gain a foothold in your network. Once inside your security perimeter, they can move around freely.

This explains why in 2024 [90% of Windows Server attacks](#) involved RDP to establish remote connections to access Windows hosts. In 2023, the number of RDP-based attacks was only 63%.

RDP-based attack on your organization's mission-critical Windows systems is a question of if and not when. Even if the latest attacks haven't hit your org, it's important not to lower your guard.

Three Types of RDP Attacks

Why Attackers Love RDP: A Breakdown of Common Exploits by Complexity



Type 1

Password-based

Abuse weak password hygiene to gain unlimited system access



Type 2

Network and Infrastructure

Exploit poor network security policies and bad configuration settings to gain unlimited access to Windows Servers and clients



Type 3

RDP Vulnerabilities

Rely on known RDP vulnerabilities and legacy systems to hijack RDP sessions

The Three Types In Detail



Type 1

Easily Preventable

How and Why Brute Force, Dictionary, and Password Spraying Attacks Exploit RDP

The [CovertNetwork-1658 \(2023\)](#) was able to launch a [password attack](#) that targeted RDP sessions. This attack exploited the fact that RDP connections pass through a specific network address called a port. In theory, a communication protocol should be able to change its default port or use a range of available ports. Most RDP sessions run over port 3389 and occasionally over [port 1098](#). This means that no matter how strong the RDP protocol becomes, potential attackers know the route taken by each RDP session. This makes it easier for hackers to gain remote access to a system by detecting and harvesting weak passwords.

The Three Types In Detail



Type 2

False Sense of Security

How and Why Default Parameters and Misconfigured Settings Help Hackers

2024's [Earth Koshchei Attack](#) took advantage of misconfigured network security. Instead of using a brute force password attack to enter the network, this attack utilized spear-phishing emails to distribute malicious RDP configuration files. This enabled them to gain direct access to local and network resources and redirect their contents to external devices.

This attack was devastatingly effective because it was able to bypass the network's authentication mechanisms. Once they entered the network, they were able to access files stored both locally and on network drives, read data from the device's clipboard, access remote servers, and exfiltrate data. What made this attack especially devastating was its sheer scope. The hackers exploited a Python-based RDP proxy called [PyRDP](#), AKA Rouge RDP, to automate the deployment and execution of their scripts.

The Three Types In Detail



Type 3

Using RDP against Itself:

How and Why Hackers Abuse RDP Vulnerabilities and Legacy Systems

In April 2025, the BlueKeep ([CVE-2019-0708](#)) exploit enabled North Korean hackers to launch an RDP attack that targeted Windows versions from XP to Server 2008 R2. It installed spyware and keyloggers on systems across South Korea and Japan.

This attack exploited the fact that RDP has been in use for nearly three decades to become enterprise computing's default remote access protocol. Over this period, hackers have been able to collect a long list of vulnerabilities. In the short term, Microsoft releases a patch to fix the issue. In the longer term, each new release of Windows Server includes improved RDP security. Unfortunately, there are reasons why an organization might prefer to keep an insecure legacy system in production rather than installing upgrades and fixes.

Implementing RDP Server Hardening

CalCom recommends:

- 01** [Unnecessary functionality compromises security](#), so all unnecessary functionality must be removed or disabled. In other words, unless you have a good reason for using RDP, you should disable it and uninstall it.
- 02** Adopt a Least-Privilege security model that grants the minimum level of permissions to those who actually require them. By extension, this approach prevents inadvertently allowing those who don't need or shouldn't have access to your IT infrastructure.
- 03** As soon as Microsoft releases them, install the latest RDP patches and service packs. When possible, install the newest version of Windows Server.



How to Harden Your Defenses Against RDP Vulnerabilities

Stopping Password Attacks

The best way to prevent password attacks, such as [CovertNetwork-1658 \(2023\)](#), is to implement these CIS benchmarks. Each Benchmark refers to a specific Windows Server policy.

Benchmark	Description	Reason	Setting(s)
1.1.1: Enforce password history	Determines the number of renewed, unique passwords associated with a user account.	Prevents the reuse or sharing of passwords.	24 or more passwords
1.1.2: Maximum password age	Sets the lifespan of a user's password in days.	The older the password, the greater the chance it can be brute-forced or compromised.	365 or fewer days, but not 0
1.1.5: Password must meet complexity requirements	Checks that new passwords meet basic strength requirements and include a mix of character types.	Popular hacking tools can easily crack weak alphanumeric passwords.	Enabled
1.1.7: Store passwords using reversible encryption	Ensures Windows encrypts user passwords.	Weakens defense against password extraction attacks.	Disabled
1.2.1: Account lockout duration	Sets the interval before unlocking a locked RDP account.	Prevents attackers from launching a DoS attack via account lockout.	15 or more minutes
1.2.2: Account lockout threshold	Defines how many failed logons trigger account lockout.	Reduces success rate of brute force attacks.	5 or fewer invalid attempts, but not 0
1.2.3: Allow Administrator account lockout	Applies Account Lockout Policy to the built-in Administrator account.	Prevents hackers from abusing an always-accessible admin account.	Enabled

Strengthening RDP Network Security

Preventing the abuse of administrator privileges, as demonstrated by the [Earth Koshchei Attack](#), is achieved by implementing effective account management policies, making it more challenging to gain access to your network infrastructure.

In addition to enforcing strong policies, you need to ensure that attackers are not able to exploit system administration tools and privileges. Next, you must ensure that hackers are not able to manipulate domain controllers. These servers control groups of machines that propagate policies across your network. Ideally, these attacks should not be able to access any host, and in the worst-case scenario, only access individual member servers. In parallel to these protective measures, you should also ensure that all network events are logged. This will show you where potential weaknesses exist, and in the event of an attack, get a complete picture of what took place, the extent of the damage, and how you can fix it.

Here are specific CIS benchmarks that will securely configure your Windows network security.

Benchmark	Description	Reason	Setting(s)
2.2.7–8: Allow log on locally	Enables RDP login from user accounts.	Accounts with this privilege have admin access, which can be abused.	Domain Controller: Administrators ENTERPRISE DOMAIN CONTROLLERS Member Server: Administrators
2.2.9–10: Allow log on through Remote Desktop Services	Enables RDP login from user accounts.	Ensures only authorized access to network devices via Remote Assistance.	Domain Controller: Administrators Member Server: Administrators, Remote Desktop Users
2.2.6–27: Allow log on through Remote Desktop Services	Prevents unauthorized local console access.	Restricts who can access systems via a local console.	Domain Controller: Guests Member Server: Guests, Local account
2.2.10.6–7: Network access — Named Pipes accessible anonymously	Controls anonymous access to network pipes.	Reduces attack surface by blocking anonymous access.	Domain Controller: LSARPC, NETLOGON, SAMR Member Server: (blank)
2.3.7.2: Set Interactive logon — Don't display last signed-in	Hides the name of the last signed-in user.	Prevents exposure of usernames to anyone with physical access.	Enabled
2.3.13.1: Allow system shutdown without login	Controls shutdown access from RDP sessions.	Prevents attackers from creating a temporary DoS by restarting systems.	Disabled
2.3.7.2 (duplicate ID?): Set Interactive logon — Logon/logoff auditing	Reports logon/logoff events from RDS sessions.	Helps investigate security incidents through auditing.	Success and Failure

Hardening RDP Servers

Ultimately, the best way to avoid an attack like [BlueKeep](#) that targets legacy RDP hosts is to install the latest version of Windows Server. Each new release includes new features and improvements that will enhance your network security. Whether you install the latest upgrade or not, you should make every effort to make sure that you deploy Microsoft's latest patches and follow their guidance.

Unfortunately, most IT organizations have to walk a fine line between improved security and the operational constraints imposed by their organization. In the worst-case scenario, deploying the latest service pack could have a similar impact on mission-critical systems as a cyber attack. This can lead to a hybrid approach where:

- New green field projects deploy the latest version of Windows
- Some projects deploy some or all of the newest service patches
- Legacy projects deploy unpatched legacy operating systems

In a hybrid environment, an organization could require RDP interoperability between projects. This is why Microsoft supports RDP [backward compatibility](#). However, older systems do not support the latest RDP security features; overall, network security will be degraded to the level of the oldest RDP version.

These benchmarks will harden your RDP servers even in an environment that supports backward compatibility.

Benchmark	Description	Reason	Setting(s)
18.10.57.3.3.3: Do not allow drive redirection	Blocks data sharing from local client drives during RDP sessions.	Prevents extraction of local data without user permission.	Enabled
18.10.57.3.3.8: Restrict clipboard transfer from server to client	Disables clipboard data transfer from RDP server to client.	Reduces system's attack surface.	Enabled: Disable clipboard transfers from server to client
18.10.57.3.9.1: Always prompt for password upon connection	Forces password prompt at start of every RDP session.	Prevents misuse of saved credentials or auto-logins.	Enabled
18.10.57.3.9.2: Require secure RPC communication	Ensures RPC traffic over RDP is encrypted and authenticated.	Protects against man-in-the-middle attacks.	Enabled
18.10.57.3.9.3: Require specific security layer for RDP connections	Enforces use of TLS to secure RDP sessions.	Secures sessions over weak connections using encryption.	Enabled: SSL
18.10.57.3.9.4: Require user authentication using NLA	Requires Network Level Authentication before RDP session starts.	Ensures only authenticated users can initiate sessions.	Enabled
18.10.57.3.9.5: Set client connection encryption level	Defines encryption strength for RDP connections.	Makes RDP sessions harder to decrypt.	Enabled: High Level

Key Takeaways

- RDP is the top attack vector for Windows systems, used in 90% of breaches in 2024.
- Poor password hygiene, misconfigurations, and legacy systems are the three main RDP attack surfaces.
- Applying CIS Benchmarks can significantly reduce exposure to brute force, lateral movement, and remote access exploits.
- Hardening RDP requires enforcing least-privilege access, blocking unnecessary features, and ensuring encrypted, authenticated sessions.
- CalCom automates RDP hardening at scale, reducing human error and accelerating secure configuration deployment.

How CalCom Can Help You

This ebook demonstrates the central role of RDP hardening in Windows Server deployments. To secure your Remote RDP infrastructure, hardening is required across your entire IT infrastructure. Manual hardening of your system across the organization can be error-prone and time-consuming. An automated hardening solution will help you achieve better results more quickly.

[CalCom's Hardening Suite](#) (CHS) is a baseline hardening solution designed to address the needs of IT operations and security teams. CHS significantly reduces operational costs and eliminates service downtime by indicating the impact of a security baseline change directly on the production environment. CHS's automated process simulates the effect of a change in a production environment, thus saving the need for testing changes in a lab environment. CHS enables you to:

- Deploy security baselines without affecting the production services.
- Reduce the costs and resources for implementing compliance.
- Manage hardening baselines for your entire infrastructure from a single point.
- Avoid configuration drifts and repeated hardening processes.

To learn more, go to our [resources page](#) and download our datasheets and white papers.

For Further Reading

[RDP Hardening and Hardening RDS Essential Guide](#)

An extensive guide to securing Windows Remote Desktop Services (RDS) by implementing critical hardening measures, including enabling Network Level Authentication (NLA), enforcing two-factor authentication, disabling redirection of printers, clipboards, COM ports, drives, LPT ports, passwords, and Plug and Play devices, and setting session timeouts.

[Remote Desktop Protocol \(RDP\) Vulnerability](#)

Microsoft's Remote Desktop Protocol (RDP) is widely used but highly targeted due to serious vulnerabilities, such as BlueKeep. These flaws can allow remote code execution, certificate spoofing, or unauthorized file access.

[RDS Clipboard Redirection: Should you allow it?](#)

Explains how Remote Desktop Services permits clipboard sharing (copy-paste) between client and server, and how hackers can exploit this vulnerability

[MadLicense CVE-2024-38077 RCE Threatens All Windows Servers](#)

MadLicense is an exploit that affects every Windows Server version from 2000 through 2025. MadLicense can gain access to remote servers by bypassing server authentication and remotely executing code via the Remote Desktop Licensing service.