

A Few More Reasons Why RDP is Insecure (Surprise!)



If it seems like Remote Desktop Protocol (RDP) has been around forever, it's because it has (at least compared to the many technologies that rise and fall within just a few years.) The initial version, known as "Remote Desktop Protocol 4.0," was released in 1996 as part of the Windows NT 4.0 Terminal Server edition and allowed users to remotely access and control Windows-based computers over a network connection.

In the intervening decades, RDP has become a widely used protocol for remote access and administration of Windows-based systems. RDP plays a crucial role in enabling remote work, IT support, and system management and has served as the foundation for various remote desktop and virtual desktop infrastructure (VDI) solutions.

The downside of RDP's widespread use is that a Remote Code Execution (RCE) vulnerability in an RDP gateway can have severe consequences, potentially leading to significant damage and compromising the security and integrity of the affected system. From an attacker's point of view, exploiting an RCE vulnerability is a way to achieve unauthorized access to the affected system, allowing them to gain control over the system, bypass security measures, and perform malicious actions that could include lateral movement, data exfiltration, malware deployment, system disruption, and more.

It's important to note that the severity of the impact will depend on various factors, including the specific vulnerability, the attacker's intent and capabilities, the targeted system's importance, and the security measures in place. Still, given the potential for unauthorized access, data breaches, and systems compromise, RCE vulnerabilities in RDP are considered a critical security concern that require immediate attention and mitigation.

Surprisingly (tongue firmly in cheek), Microsoft has recently published security bulletins for exactly such a scenario. Please patch!

DLL Hijacking Used to Exploit RDP - [CVE-2023-24905#](#)

Leveraging dynamic link library (DLL) hijacking, the RDP client was compromised when it tried to load a file from the current working directory (CWD) instead of the Windows OS directory.

[From the researcher's blog:](#)

"It became clear that we could spoof resources loaded by changing the icons and strings in the DLL, which would present an interesting phishing attack vector. In this scenario, an attacker could manipulate the visual elements, such as icons and strings within the DLL, to mislead the user into performing certain actions. For example, by changing the icons and strings, an attacker could make an error message look like a legitimate system notification or transform a dangerous action (such as downloading a file) into something seemingly harmless (like performing a software update)."

The RCE comes from changing the DLL string to a malicious file, placing it in a commonly accessed file sharing location, and then tricking a user into running it. Interestingly, this exploit only affected devices running Windows OS on advanced RISC machines (ARM) processors. Both RDP & Windows OS on ARM are commonly used in industrial control systems (ICS) and other operational technology (OT) environments, making industrial enterprises and critical infrastructure a prime target of this exploit.

RDP Gateway Vulnerability Could Threaten Compliance - [CVE-2023-35332#](#)

Under normal operation, the RDP Gateway protocol creates a primary secure channel using the Transport Control Protocol (TCP) and Transport Layer Security (TLS) version 1.2, a widely accepted protocol for secure communication. ***Additionally, a secondary channel is established over user datagram protocol (UDP), implementing datagram transport layer security (DTLS) 1.0.*** It is important to recognize that DTLS 1.0 has been deprecated since March 2021 due to well-known vulnerabilities and security risks.

[From the researcher's blog:](#)

"This RDP Gateway vulnerability presents both a substantial security risk and a significant compliance issue. The use of deprecated and outdated security protocols, such as DTLS 1.0, may lead to inadvertent non-compliance with industry standards and regulations."

The secondary UDP channel is concerning, especially since it uses a protocol with many known issues (DTLS 1.0). The biggest challenge is that operators may not even know that they are out of compliance with this outdated protocol.

Conclusion

To avoid the consequences of these vulnerabilities, the best thing to do is to update your RDP clients and gateways with the patches Microsoft has released. But inevitably, there will be other RCEs on RDP, and that means a crucial next step is to get ahead of threat actors by deploying robust access controls. Because RDP is widely used in OT/ICS environments that are all but [impossible to patch](#), it's especially important that organizations running these systems [find security tools](#) that meet their special requirements regarding systems availability, operational safety, and more.

Found this article interesting? This article is a contributed piece from one of our valued partners.
Follow us on [Twitter](#)  and [LinkedIn](#) to read more exclusive content we post.