Another reason to hurry with Windows server patches: A new RDP vulnerability



Enlarge / A crafted request is like a skeleton key for gaining access to unpatched Windows Remote Desktop servers.
Anadolu Agency / Getty Images

reader comments

36 with 29 posters participating

Share this story

While much of the attention around Microsoft's latest Windows security patch has been focused on a flaw in Windows 10 and Windows Server that could be used to spoof a certificate for secure Web sessions or signing code, there were 48 other vulnerabilities that were fixed in the latest update package. Five were related to Microsoft's Remote Desktop Protocol

(RDP)-based service, which is used by thousands of organizations for remote access to computers within their networks. And two of them are flaws in the Windows Remote Desktop Gateway that could allow attackers to gain access to networks without having to provide a login.

These two separate bugs, identified as CVE-2020-0609 and CVE-2020-0610, are rated as more dangerous than the crypto bug by Microsoft because, while they're not yet exploited, they could be used to remotely execute code on targeted RDP servers before the gateway even attempts to authenticate them.

"An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights," the Microsoft Security Response Center summary of both vulnerabilities warned. And there is no way to work around the vulnerability without applying a software update. Both attacks rely on specially crafted requests to the Remote Desktop Gateway using the RDP protocol.

Remotely Desktop Pwnable

These new vulnerabilities are unique from—but similar in impact to—the Remote Desktop Service vulnerability revealed last May, also labeled as critical by Microsoft. Multiple proof-of-concept exploits of the bug, dubbed "Bluekeep," quickly emerged, and the exploit was potentially "wormable"—meaning that it could be used to infect systems that could then in turn scan for other vulnerable systems to attack. According to some researchers, an exploit for the vulnerability had been on sale on Web criminal marketplaces since September of 2018. A cursory search on the security search engine Shodan showed hundreds of systems that are still potentially exposed by that vulnerability.

The other vulnerabilities patched in the latest release from Microsoft related to RDP include a flaw in Remote Desktop Web Access that could allow an attacker using Web requests to

obtain legitimate users’ login credentials, a denial of service vulnerability in RDP Gateway, and a flaw in the Windows Remote Desktop Client across all supported versions of Windows (including Windows 7) that could allow a malicious remote RDP server to execute code remotely on the client machine.

Given the slower rate of patching that usually occurs with servers—particularly older servers—these new vulnerabilities may have a long life as well. And depending on how deep their roots are, Microsoft may be forced to extend the patches to older operating systems as well. The May 2019 bug’s impact was judged to be so severe that it led Microsoft to issue updates even for Windows XP, Vista, and Server 2003.

https://arstechnica.com/?p=1644525