Security Advisory Report - OBSO-1905-02

Microsoft Windows Remote Desktop Services RDP Connection Request Handling Remote Code Execution (CVE-2019-0708)

Release Date: 2019-05-17 09:14:09
Last Update: 2019-05-17 09:14:09

Summary

Microsoft Windows contains a flaw in **Remote Desktop Services** that is triggered during the handling **of a specially crafted request from an RDP connection**.

This may **allow a remote attacker to potentially execute arbitrary code.**

This vulnerability may be exploited by malware, so it can be exploited in a way similar to the **WannaCry**.

Details

Customers are advised to update with the latest Microsoft patches their Windows installations.

Please note that because of the severity of this vulnerability Microsoft provides patches even for older Windows systems which are no officially supported (see references).

In the case where patching is not possible Microsoft provides some Mitigations and Workarounds which can be found in Microsoft's Security Advisory and indicate the following :

"

Mitigations

The following mitigation may be helpful in your situation. In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as possible even if you plan to leave Remote Desktop Services disabled:

1. Disable Remote Desktop Services if they are not required.

If you no longer need these services on your system, consider disabling them as a security best practice. Disabling unused and unneeded services helps reduce your exposure to security vulnerabilities.

Workarounds

The following workarounds may be helpful in your situation. In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as possible even if you plan to leave these workarounds in place:

1. Enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2

You can enable Network Level Authentication to block unauthenticated attackers from exploiting this vulnerability. With NLA turned on, an attacker would first need to authenticate to Remote Desktop Services using a valid account on the target system before the attacker could exploit the vulnerability.

2. Block TCP port 3389 at the enterprise perimeter firewall

TCP port 3389 is used to initiate a connection with the affected component. Blocking this port at the network perimeter firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. This can help protect networks from attacks that originate outside the enterprise perimeter. Blocking the affected ports at the enterprise perimeter is the best defense to help avoid Internet-based attacks. However, systems could still be vulnerable to attacks from within their enterprise perimeter.

"

Affected Products

Unify has products which run in Windows environments.

Customers are advised to follow their standard patching processes to apply the official Microsoft patches for this vulnerability.

Recommended Actions

Patch Windows installations.

If not possible follow mitigations as described by Microsoft

References

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
- https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708
- https://www.huawei.com/en/psirt/security-notices/2019/huawei-sn-20190515-01-windowsrdp-en
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-0708
- https://github.com/rockmelodies/CVE-2019-0708-Exploit
- https://krebsonsecurity.com/2019/05/microsoft-patches-wormable-flaw-in-windows-xp-7-and-windows-2003/

Advisory: OBSO-1905-02, status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com