# Product Security Information

Vulnerability for Windows Remote Desktop Services (RDP) Remote Code Execution

BOSCH-SI-2019-0903-BT

CVE-2019-1181/1182 (CVSS v3 Base Score: 9.8)

## 1 Overview

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests.

## 2 Technical Details

### 2.1 Considered Common Vulnerability and Exposure (CVE)

CVE-2019-1181/1182 (CVSS: 9.8) Remote Desktop Services Remote Code Execution Vulnerability
Further information on this vulnerability can be found at
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181 and
https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/

### 2.2 Exploitability

This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

A prerequisite for a successful attack is network access to the RDP service on port 3389 on the targeted Windows operating system. Firewalled and systems with the latest security updates are not vulnerable.

## 3 Bosch products

Bosch relies on a Microsoft Windows operating system for several products. Consequently, some devices are affected by the corresponding vulnerability. Depending on the products category, different configurations may be distinguished.

Category A: Directly affected devices, by default reachable via network on the vulnerable RDP Port 3389.

- DIVAR IP 3000
- DIVAR IP 6000
- DIVAR IP 7000
- DIVAR IP all-in-one 5000
- HP Workstation
- HP Server DL380

Category B: Devices shipped by default with deactivated RDP, which can be re-enabled by the customer.
► DIVAR IP 2000
► DIVAR IP 5000
► UGM 2040 plus

Category C: Devices shipped with disabled RDP services and additional firewall rules.
► VIDEOJET decoder 7000
► VIDEOJET decoder 8000

## 4 Vulnerability fix and mitigation

It is recommended for any Bosch device to update its operating system and supported firmware to the latest patch level.

For products of each category, an individual approach is advised:

► Category A: Please log into the system with an administrative account (e.g. BVRAdmin) and install the CVE-2019-1181 patch either manually from the Microsoft website or via the auto update feature of the operating system.

► Category B: Please deactivate the devices debugging RDP service. Use the debugging feature only in a secure network environment. The necessary operating system patches will be included in the next firmware release.

► Category C: The RDP service is not accessible in any configuration. No action or fix is required.

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

## 5 Document Change Log

2019.09.03 – Revision 1.00: Initial Release