Product Security Information

Vulnerability for Windows Remote Desktop Services (RDP) Remote Code Execution - 2019 June 12th
CVE-2019-0708 (CVSS: 9.8)

1 Overview

On May 14th 2019, information related to the Remote Desktop Services Remote Code Execution Vulnerability of Microsoft Windows operating system was published. The flaw affects the following operating systems used by Bosch Security and Safety systems products:

- Windows 7 (32-bit/x64)
- Windows Server 2008 (32-bit/x64/Itanium)
- Windows Server 2008 R2 (32-bit/x64/Itanium)

2 Technical details

2.1 Considered Common Vulnerability and Exposure (CVE)

CVE-2019-0708 (CVSS: 9.8): Remote Desktop Services Remote Code Execution Vulnerability

2.2 Exploitability

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 (only with WSS 2008 R2)
- DIVAR IP 7000 (only with WSS 2008 R2)
- HP Workstation (only with Windows 7)
- HP Server DL380 (only with Windows Server 2008 R2)

Category B: Devices shipped by default with deactivated RDP, which can be re-enabled by the customer.

- DIVAR IP 2000

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. Microsoft provides for this vulnerability additional information on its homepage (Link). 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-2019-0708 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.