rexroth
A Bosch Company

Security Advisory

Remote Desktop Services Remote Code Execution Vulnerability in Rexroth Industrial PCs

1 Advisory Information

Advisory ID: BOSCH-SA-856281
CVSSv3 Base Score:

- CVE-2019-0708
  - CVSS 3.0: 9.8 (Critical)
- **Published:** 13 Oct 2020
- **Last Updated:** 13 Oct 2020

2 Summary

Microsoft has published information [1] for several versions of Microsoft Windows XP, Microsoft Windows XP embedded, Microsoft Windows 7 and Microsoft Windows 7 Embedded Standard, regarding a vulnerability in the Remote Desktop Service. The vulnerability could allow an unauthenticated remote attacker to execute arbitrary code on the target system if the system exposes the service to the network.
Rexroth Industrial PCs on these operating systems are affected by this vulnerability.

3 Affected Products

- Rexroth VEP15.6
- Rexroth VEP21.6
- Rexroth VEP30.5
- Rexroth VEP40.5
- Rexroth VEP50.5
- Rexroth VPB40.3
- Rexroth VPB40.4
- Rexroth VPP16
- Rexroth VPP40
- Rexroth VPP60

4 Solution

4.1 Software Update

Microsoft has released patches closing this vulnerability [2], [3]. It is recommended that the appropriate patch for the operating system should be installed in a timely manner, if possible.

4.2 Compensatory Measures

In use cases in which a device update is not possible or not yet available, compensatory measures are recommended which prevent or at least complicate taking advantage of the vulnerability. Always define such compensatory measures individually, in the context of the operational environment. Some possible measures are described in the “Security Manual Electric Drives and Controls”, for example the network segmentation (please see [4]). In general, it is highly recommended to implement the measures described in the “Security Manual Drives and Controls”.

5 Vulnerability Details

5.1 CVE-2019-0708

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.
CVE description: 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, aka ‘Remote Desktop Services Remote Code Execution Vulnerability’.

- Problem Type:
  - Remote Code Execution
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C
  - Base Score: 9.8 (Critical)
  - Temporal Score: 9.4 (Critical)

5.2 Remark

Vulnerability classification has been performed using the CVSS v3.1 scoring system. The CVSS environmental score is specific to each customer’s environment and should be defined by the customer to attain a final scoring.

6 Additional Resources

[1] Microsoft Advisory for CVE-2019-0708:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
[2] Microsoft Update Catalog KB4500331 Windows XP:
https://www.catalog.update.microsoft.com/Search.aspx?q=KB4500331%20Windows%20XP
[3] Microsoft Update Catalog KB4499175:
https://www.catalog.update.microsoft.com/Search.aspx?q=KB4499175
[4] Bosch Rexroth Security Manual Electric Drives and Controls:
https://www.boschrexroth.com/various/utilities/mediadirectory/download/index.jsp?object_nr=R911342562

7 Revision History

13 Oct 2020: Initial Publication