1 Advisory Information

- **Advisory ID:** BOSCH-SA-363824-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2017-0144
    - Base Score: 8.1 (High)
  - CVE-2019-0708
    - Base Score: 9.8 (Critical)
  - CVE-2020-6774
    - Base Score: 9.3 (Critical)
- **Published:** 27 May 2020
- **Last Updated:** 27 May 2020

2 Summary

Several issues have been discovered affecting the Bosch Recording Station (BRS). The critical issues apply to BRS systems which are connected to an open network.

Bosch strongly recommends to operate the BRS system in a closed network and prevent unauthorized direct access to the BRS server.

The product was announced end of life in 2016.

3 Affected Products

- Bosch Recording Station

4 Solution and Mitigations

4.1 Restricted Physical Access

The hardware access to the system should be heavily restricted and be locked for public.

4.2 Limited User Exposure

The application usage itself should be limited to a trusted user environment and the system logs need to be checked regularly.

4.3 Closed Network

Bosch strongly recommends to operate the BRS in a closed network with very limited access to the system. The services SMB and RDP should be deactivated to mitigate the risk for vulnerabilities CVE-2017-0144 and CVE-2019-0708.

4.4 Upgrade hardware

Customers who want to operate their appliance in an open network are strongly advised to update their BRS to the DIVAR IP all-in-one 5000.

5 Vulnerability Details

5.1 CVE-2017-0144

The Bosch Recording Station is affected by the “EternalBlue” vulnerability due to the usage of Windows 7.

CVE description: The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka “Windows SMB Remote Code Execution Vulnerability.” This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

- Problem Type:
  - Remote Code Execution
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.1 (High)

5.2 CVE-2019-0708

The Bosch Recording Station is affected by the “BlueKeep” vulnerability due to the usage of Windows 7.

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
  - Base Score: 9.8 (Critical)

5.3 CVE-2020-6774

CVE description: Improper Access Control in the Kiosk Mode functionality of Bosch Recording Station allows a local unauthenticated attacker to escape from the Kiosk Mode and access the underlying operating system.

- Problem Type:
  - CWE-284 Improper Access Control
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
  - Base Score: 9.3 (Critical)

5.4 Lack of Full Disk Encryption

The Bosch Recording Station does not support Full Disk Encryption. An attacker with physical access to the system could physically remove the system drive and read and modify contents of the file system.

- Problem Type:
  - CWE-311 Missing Encryption of Sensitive Data
- CVSS Vector String: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 6.8 (Medium)

5.5 Remark

Vulnerability classification has been performed using the CVSSv3 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] Bosch Building Technologies Security Advisory page : https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Please contact the Bosch PSIRT if you have feedback, comments, or additional information about this vulnerability at: psirt@bosch.com.

7 Revision History

- 27 May 2020: Initial Publication

8 Appendix

8.1 Material List: Bosch Recording Station

Family Name	CTN	SAP#	Material description
Bosch Recording Station	BRS-TOW-1100A	F.01U.246.997	BRS Tower 1TB
Bosch Recording Station	BRS-TOW-4100A	F.01U.246.998	BRS Tower 4TB
Bosch Recording Station	BRS-RAC1-4100A	F.01U.246.999	BRS 1U 19" Rack-mount 4TB
Bosch Recording Station	BRS-RAC2-8100A	F.01U.247.000	BRS 2U 19" Rack-mount 8TB
Bosch Recording Station	BRS-RAC2-8200A	F.01U.247.002	BRS 2U 19" Rack-mount 16TB