Miele Product Security Bulletin

# Information on Microsoft Remote Desktop Services Remote Code Execution Vulnerability (CVE-2019-0708)

| Issued: | 28.05.2019 |
|---|---|
| Bulletin No: | MPSB-2019-002 |
| Issuer: | Miele PSIRT, psirt@miele.com |
| Classification | Public |

## Affected Products

| Product | Software Version |
|---|---|
| PS5XXX | Systems running Windows XP and Windows 7 that have not been updated during our last field corrective action in June 2018. |

## Vulnerability Type

Improper Input Validation (CWE-20)

## Summary

On May 14th Microsoft released a patch for a critical vulnerability (CVE-2019-07-08) in the Microsoft RDP service (Remote Desktop Service) running on Windows XP and Windows 7.

The vulnerable Microsoft service is installed on our PS5XXX Series sterilizers (Windows XP and Windows 7 version). However, during our last field corrective action we deactivated the service. Therefore, the vulnerability can not be exploited and it is not required to install the patch. However, customers where the corrective action has not taken place yet or will never take place[1], are affected by the vulnerability. This is because the service on those devices is still active and could be exploited by an attacker.

Other Miele products are not affected by the vulnerability.

## References

- Microsoft Information: https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708

---

[1] The field corrective action was and is optional for every European customer.

# Miele Product Security Bulletin

- Information on Miele field corrective action: https://www.bfarm.de/SharedDocs/Kundeninfos/DE/02/2018/02863A-18_kundeninfo_de.pdf?__blob=publicationFile&v=3
- BSI information: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Windows-Schwachstelle-RDP-150519.html