

## **SSA-932041: Vulnerability in Radiography and Mobile X-ray Products from Siemens Healthineers**

Publication Date: 2019-05-24  
Last Update: 2019-05-24  
Current Version: V1.0  
CVSS v3.0 Base Score: 9.8

### **SUMMARY**

Microsoft has released updates for several versions of Microsoft Windows, which fix 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.

Some Radiography and Mobile X-ray products from Siemens Healthineers are affected by this vulnerability. The exploitability of the vulnerability depends on the actual configuration and deployment environment of each product.

Siemens Healthineers recommends contacting Siemens Healthineers service desk.

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
AXIOM Multix M: All versions with Canon detector	Contact Siemens Regional Support Center.
AXIOM Vertex MD Trauma: All versions with Canon detector	Contact Siemens Regional Support Center.
AXIOM Vertex Solitaire M: All versions with Canon detector	Contact Siemens Regional Support Center.
MOBILETT XP Digital: All versions with Canon detector	Contact Siemens Regional Support Center.
MULTIX PRO ACSS P: All versions with Canon detector	Contact Siemens Regional Support Center.
MULTIX PRO P: All versions with Canon detector	Contact Siemens Regional Support Center.
MULTIX PRO/PRO ACSS/PRO Navy: All versions with Canon detector	Contact Siemens Regional Support Center.
MULTIX Swing: All versions with Canon detector	Contact Siemens Regional Support Center.
MULTIX TOP: All versions with Canon detector	Contact Siemens Regional Support Center.

MULTIX TOP ACSS: All versions with Canon detector	Contact Siemens Regional Support Center.
MULTIX TOP P/TOP ACSS P: All versions with Canon detector	Contact Siemens Regional Support Center.
VERTIX SOLITAIRE: All versions with Canon detector	Contact Siemens Regional Support Center.

## **WORKAROUNDS AND MITIGATIONS**

Siemens Healthineers has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- If possible, block port 3389/tcp on an external firewall.
- Secure the surrounding environment according to the recommendations provided by Microsoft to minimize the risk.

## **GENERAL SECURITY RECOMMENDATIONS**

In addition, Siemens Healthineers recommends the following:

- Ensure you have appropriate backups and system restoration procedures.
- For specific patch and remediation guidance information, contact your local Siemens Healthineers customer service engineer, portal or our Regional Support Center.

## **PRODUCT DESCRIPTION**

Siemens Healthineers Radiography and Mobile X-ray systems are used in clinical environments for medical imaging using X-ray.

## **VULNERABILITY CLASSIFICATION**

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (<https://www.first.org/cvss/>). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

### Vulnerability CVE-2019-0708

An unauthenticated attacker with access to port 3389/tcp in an affected device may execute arbitrary commands with elevated privileges.

The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected device. No user interaction is required to exploit this vulnerability. The vulnerability impacts the confidentiality, integrity, and availability of the affected device.

CVSS v3.0 Base Score      9.8  
CVSS Vector              CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

## **ADDITIONAL INFORMATION**

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

<https://www.siemens.com/cert/advisories>

## **HISTORY DATA**

V1.0 (2019-05-24): Publication Date

## **TERMS OF USE**

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website ([https://www.siemens.com/terms\\_of\\_use](https://www.siemens.com/terms_of_use), hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.