SSA-616199: BlueKeep Vulnerability Identified in RAPIDPoint® 500 Operating on Windows XP

Publication Date:	2019-05-24
Last Update:	2020-01-14
Current Version:	V1.2
CVSS v3.1 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.

RAPIDPoint® 500 systems operating on Windows XP are affected by this vulnerability.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RAPIDPoint® 500: Version 2.3.2 and earlier	The software update to V2.3.3 will be installed on the next service visit or an appointment will be scheduled to update the system(s).

WORKAROUNDS AND MITIGATIONS

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

- Configure your external firewall to block port 3389/tcp if not already done.
- Secure the surrounding environment according to the recommendations provided by Microsoft to minimize the risk.
- Ensure you have appropriate backups and system restoration procedures.

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 Healthcare Diagnostics provides point-of-care products and services that enable healthcare providers to render better patient management and help ensure optimized clinical outcomes.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

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 v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

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
V1.1 (2019-07-09):	Removed AUWi and AUWi Pro, changed patch release date
V1.2 (2020-01-14):	Added patch availability, added CVSS v3.1 score

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, 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.