SSA-553445: DNS “Name:Wreck” Vulnerabilities in Multiple Siemens Energy AGT and SGT solutions

Publication Date: 2021-08-10
Last Update: 2021-08-10
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

One of the DNS-related vulnerabilities that were reported as “Name:Wreck” may affect the following Siemens Energy products:

- Industrial Gas Turbines SGT-100, SGT-200, SGT-300 and SGT-400 with Allen Bradley control systems
- Aeroderivative Gas Turbines SGT-A20, SGT-A35 and SGT-A65 with FT125 control systems

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SGT-100: All versions	As only Rockwell Automation / Allen Bradley components are affected, please see Rockwell Security Advisory PN1564 for affected parts and software/firmware updates. Some updates may not be compatible with other components in the system. Contact Siemens Energy for further support.
SGT-200: All versions	As only Rockwell Automation / Allen Bradley components are affected, please see Rockwell Security Advisory PN1564 for affected parts and software/firmware updates. Some updates may not be compatible with other components in the system. Contact Siemens Energy for further support.
SGT-300: All versions	As only Rockwell Automation / Allen Bradley components are affected, please see Rockwell Security Advisory PN1564 for affected parts and software/firmware updates. Some updates may not be compatible with other components in the system. Contact Siemens Energy for further support.
SGT-400: All versions	As only Rockwell Automation / Allen Bradley components are affected, please see Rockwell Security Advisory PN1564 for affected parts and software/firmware updates. Some updates may not be compatible with other components in the system. Contact Siemens Energy for further support.

SGT-A20: All versions	As only Rockwell Automation / Allen Bradley components are affected, please see Rockwell Security Advisory PN1564 for affected parts and software/firmware updates. Some updates may not be compatible with other components in the system. Contact Siemens Energy for further support.
SGT-A35: All versions	As only Rockwell Automation / Allen Bradley components are affected, please see Rockwell Security Advisory PN1564 for affected parts and software/firmware updates. Some updates may not be compatible with other components in the system. Contact Siemens Energy for further support.
SGT-A65: All versions	As only Rockwell Automation / Allen Bradley components are affected, please see Rockwell Security Advisory PN1564 for affected parts and software/firmware updates. Some updates may not be compatible with other components in the system. Contact Siemens Energy for further support.

WORKAROUNDS AND MITIGATIONS

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

- While firmware updates are suggested in the original advisory as solutions, the updates may not be compatible with the software or other components in the system. Please contact your local Siemens Energy representative for an assessment.
- For more details on how to mitigate this vulnerability, see Rockwell Security Advisory PN1564 (https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1131196, Login required)

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs or DSOs) worldwide are usually required by regulations to build resilience into the power grids by applying multi-level redundant secondary protection schemes. It is therefore recommended that the operators check whether appropriate resilient protection measures are in place. The risk of cyber incidents impacting the grid's reliability can thus be minimized by virtue of the grid design.

Siemens strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment.

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

Siemens gas turbines are suitable for a wide range of applications. They can be used for power generation applications for utilities, independent power producers, oil and gas, and industrial users, such as chemicals, pulp and paper, food and beverage, sugar, automotive, metalworking, mining, cement, wood processing, and textiles. They are also used in mechanical drive applications for oil and gas, and chemical industry.

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-2016-20009

** UNSUPPORTED WHEN ASSIGNED ** A DNS client stack-based buffer overflow in ipdnsc_decode_name() affects Wind River VxWorks 6.5 through 7. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

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:U/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

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 (2021-08-10): 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, 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.