SSA-736385: Memory Corruption Vulnerability in OpenV2G

Publication Date:	2022-05-10
Last Update:	2022-05-10
Current Version:	V1.0
CVSS v3.1 Base Score:	6.2

SUMMARY

The open source software OpenV2G contains a buffer overflow vulnerability that could allow an attacker to trigger a memory corruption.

Siemens has released an update for the OpenV2G and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
OpenV2G: V0.9.4	Update to V0.9.5 or later version https://sourceforge.net/projects/openv2g/

WORKAROUNDS AND MITIGATIONS

Product specific remediations or mitigations can be found in the section Affected Products and Solution.

Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

The OpenV2G project provides an open source implementation of the latest draft of the ISO/IEC Vehicle-to-Grid Communication Interface (V2G CI) standard. Based on the OpenV2G library you are able to exchange the standardised XML-based messages between a Plug-In Electrical Vehicle (PEV) and an Electric Vehicle Supply Equipment (EVSE).

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-2022-27242

The OpenV2G EXI parsing feature is missing a length check when parsing X509 serial numbers. Thus, an attacker could introduce a buffer overflow that leads to memory corruption.

CVSS v3.1 Base Score	6.2
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Philipp Spiegelt, Patrick Hochscheidt, and Steffen Sanwald from Mercedes-Benz Tech Innovation for reporting the vulnerability

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 (2022-05-10): 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.