SSA-400332: Insufficient Design IP Protection in IEEE 1735 Recommended Practice - Impact to Questa and ModelSim

Publication Date: 2021-12-14
Last Update: 2022-11-08
Current Version: V1.1
CVSS v3.1 Base Score: 9.0

SUMMARY

A security research [1] identified weaknesses in the IEEE 1735 recommended practice for encryption of Design IP, which could allow a sophisticated attacker access to unencrypted Design IP data in IEEE 1735-compliant products. This advisory addresses the specific details for the affected Siemens software products: Questa and ModelSim simulators.

Siemens is preparing updates and recommends specific countermeasures for Questa and ModelSim.

[1] https://arxiv.org/abs/2112.04838

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
ModelSim Simulation: All versions	Update to new releases as they become available (see also section Additional Information) https://support.sw.siemens.com/en-US/product/852852093/ See further recommendations from section Workarounds and Mitigations
Questa Simulation: All versions	Update to new releases as they become available (see also section Additional Information) https://support.sw.siemens.com/en-US/product/852852103/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Company-internal use of encrypted design IP data: Apply technical and procedural measures to ensure that access to the data is granted on a need-to-know basis.
- Companies that deliver encrypted design IP data to their customers: ensure that procedural and contractual measures are in place that minimize the risk of unauthorized access to the data.

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

Questa and ModelSim simulators are used worldwide to simulate, debug, and verify integrated circuit designs, enabling design and verification engineering team to accelerate time-to-market of high-quality, high-complexity ASIC and FPGA designs.

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-2021-42023

The RSA white-box implementation in affected applications insufficiently protects the built-in private keys that are required to decrypt electronic intellectual property (IP) data in accordance with the IEEE 1735 recommended practice.

This could allow a sophisticated attacker to discover the keys, bypassing the protection intended by the IEEE 1735 recommended practice.

CVSS v3.1 Base Score	9.0
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N/E:P/RL:U/RC:C
CWE	CWE-522: Insufficiently Protected Credentials

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Julian Speith and Christof Paar from Max Planck Institute for Security and Privacy (MPI-SP) for coordinated disclosure
- Florian Schweins and Alexander May from Ruhr University Bochum (RUB) for coordinated disclosure

ADDITIONAL INFORMATION

Siemens is addressing the issue in multiple phases. Questa Simulation and ModelSim Simulation are being enhanced to contain improved design IP protection over several releases, including the use of new keys, during 2022 and 2023.

Significant changes in version 2022.4 (released October 2022):

- Support of customer-specific symmetric keys according to IEEE 1735
- Improvement of the white-box implementation
- Changed RSA private keys

For more information customers can refer to the related article in the support portal:

- ModelSim: https://support.sw.siemens.com/en-US/product/852852093/knowledge-base/MG618380
- Questa: https://support.sw.siemens.com/en-US/product/852852103/knowledge-base/MG618380

The relevant research paper, titled “How Not to Protect Your IP – An Industry-Wide Break of IEEE 1735 Implementations” is available at https://arxiv.org/abs/2112.04838.

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 (2021-12-14): Publication Date
V1.1 (2022-11-08): Added significant changes implemented in latest product version 2022.4

TERMS OF USE