



INTEL-SA-00117

THE LATEST SECURITY INFORMATION ON INTEL[®] PRODUCTS.

[Report a Vulnerability](#) [Product Support](#)

INTEL[®] SGX SDK EDGER8R AND INTEL[®] SOFTWARE GUARD EXTENSIONS PLATFORM SOFTWARE COMPONENT

Intel ID:	INTEL-SA-00117	USA (English)   
Product family:	Intel® SGX	
Impact of vulnerability:	Elevation of Privilege	
rating:	Severity	Important
Original release:	Mar 20, 2018	
Last revised:	July 23, 2019	

Summary:

CVE-2018-3626: The Edger8r tool in the Intel® Software Guard Extensions (SGX) Software Development Kit (SDK) before version 2.1.2 (Linux) and 1.9.6 (Windows) may generate code that is susceptible to a side channel attack, potentially allowing a local user to access unauthorized information.

CVE-2017-5736: An elevation of privilege in Intel® Software Guard Extensions Platform Software Component before 1.9.105.42329 allows a local attacker to execute arbitrary code as administrator.

Description:

CVE-2018-3626: Recently it was reported that the Edger8r Tool, a software component of the Intel® Software Guard Extensions (SGX) Software Development Kit (SDK), may generate C source code potentially leading to a software based side-channel vulnerability.

Exposure of the vulnerability is limited to enclaves produced by developers who use the '*string*' attribute or the '*sizefunc*' attribute in the Edger8r Enclave Definition Language (EDL) syntax. When these attributes are used, and the resultant code is compiled into an SGX enclave, then that enclave may be exposed to a side-channel which could reveal sensitive data within the enclave. The actions outlined in this document should be followed to help minimize potential impacts.

The issue has the following Computer Vulnerability Scoring System (CVSS) rating

› 4.0 Medium CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE-2017-5736: An elevation of privilege in Intel® Software Guard Extensions Platform Software Component before 1.9.105.42329 allows a local attacker to execute arbitrary code as administrator.

› 8.2 High CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H




Affected products:

CVE-2018-3626: Products developed with Intel® SGX SDK before version 2.1.2 (Linux) and 1.9.6 (Windows)

CVE-2017-5736: Intel® Software Guard Extensions Platform Software Component before 1.9.105.42329

Recommendations:

CVE-2018-3626: Intel recommends that SGX developers, ISVs, and other affected parties review the information below, and undertake the related actions necessary to enhance their platform security.

USA (English)   

- › Update Intel® SGX SDK to version 2.1.2 (Linux Hotfix release) or 1.9.6 (Windows SDK & PSW). Intel released the updated SDKs, beginning March 16, 2018. Use of the most current SGX SDK ensures the most up to date support for SGX and its applications.
- › Developers should recompile and re-issue their enclaves with the updated Intel SGX SDK which became available on March 16, 2018 for Windows and Linux.
- › If an SGX enclave developer is using the 'string' and/or 'sizefunc' attributes in their enclave interface, the developer should review the technical guidance and determine whether they should rebuild enclave projects using the updated SDK.
- › Additional guidance can be found in the whitepaper "Intel® Software Guard Extensions (SGX) SW Development Guidance for Potential Edger8r Generated Code Side Channel Exploits
- › An updated "Intel® Software Guard Extensions (SGX) SW Development Guidance for Potential Bounds Check Bypass (CVE-2017-5753) Side Channel Exploits" has also been released based on changes made to the EDL syntax by this issue.
- › Developers implementing their own SDK should review the documentation and code changes issued with the Intel SGX SDK for Linux.

If attestation is used

One way to ensure that SGX platforms are up to date is through the process of attestation. The attestation process verifies that the platform is a valid SGX platform and the platform components meet a defined set of security requirements. In addition, the attestation process enables the application provider to verify the security version of the application.

CVE-2017-5736: Intel highly recommends that developers and users update to Intel® Software Guard Extensions Platform Software Component version 1.9.105.42329 or later.

For Windows 10 users run Windows update and version 1.9.105.42329 will be updated.




For developers an updated client has been posted here: <https://software.intel.com/en-us/sgx-sdk/download>

Acknowledgements:

Intel would like to thank Jo Van Bulck, Frank Piessens, and Raoul Strackx of Ku Leuven University for reporting CVE-2018-3626 and working with us on coordinated disclosure.

CVE-2017-5736 was found via Internal Validation.

Intel would also like to thank employees Kekai Hu, Ke Sun, Henrique Kawakami and Rodrigo Branco for CVE-2018-3626 and CVE-2017-5736.

USA (English)   

Revision History

Revision	Date	Description
1.0	19-March-2018	Initial Release
1.1	20-March-2018	Fix CVE Number
1.2	23-July-2019	Updated Acknowledgements

CVE Name: CVE-2018-5736

Legal Notices and Disclaimers

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at <https://intel.com>.




Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.
Copyright © Intel Corporation 2019

Report a Vulnerability

If you have information about a security issue or vulnerability with an **Intel branded product or technology**, please send an e-mail to secure@intel.com sensitive information using our PGP public key

USA (English)   

Please provide as much information as possible, including:

- › The products and versions affected
- › Detailed description of the vulnerability
- › Information on known exploits

A member of the Intel Product Security Team will review your e-mail and contact you to collaborate on resolving the issue. For more information on how Intel works to resolve security issues, see:

- › Vulnerability handling guidelines

For issues related to Intel's external web presence (Intel.com and related subdomains), please contact Intel's External Security Research team.

Need product support?

The secure@intel.com security issues.


e-mail address should only be used for reporting

If you...

- › Have questions about the security features of an Intel product
- › Require technical support
- › Want product updates or patches

Please visit [Support & Downloads](#)

Company Information

 Commitment

USA (English)   

Communities

Investor Relations

Contact Us

Newsroom

Jobs



© Intel Corporation

Terms of Use

*Trademarks

Privacy

Cookies

Supply Chain Transparency

Site Map