# Intel® SGX Linux Advisory

| | |
|---|---|
| Intel ID: | INTEL-OSS-10004 |
| Product family: | Intel® Software Guard Extensions Platform Software Component |
| Imact of vulnerability: | Denial of Service |
| Severity rating: | Important |
| Original release: | 03/16/2018 |
| Last revised: | 03/16/2018 |
| CVE: | CVE-2018-3689 |

## SUMMARY

Vulnerabilities in SGX Linux SW allow unprivileged user with local access to create a denial of service that can affect all users of SGX.

## DESCRIPTION

There are vulnerabilities in the Intel Architectural Enclave Service Manager (AESM) for Linux that can result in, effectively, AESM being disabled. AESM is key component for the remote attestation of enclaves. The vulnerability can be exploited by an unprivileged user in a potentially multiuser / server environment, thus effectively disabling Intel® SGX attestation for any other user of the affected server. In a multi-VM setting, this affects SGX solely in the VM running the AESM instance being attacked.

The vulnerabilities can result in Denial of Service of the AESM and, as a result, of SGX remote attestation. SGX data confidentiality or integrity is not compromised by this exploit.

## AFFECTED PRODUCTS

Intel® Software Guard Extensions Platform Software Component for Linux before 2.1.102.

## RECOMMENDATIONS

Upgrade to Intel® Software Guard Extensions Platform Software Component for Linux 2.1.102 or later.

## ACKNOWLEDGEMENTS

Intel would like to thank Michael N. Henry and Alexander Gutkin of Intel DCG Red Team for reporting this issue and working with us on coordinated disclosure.

## REVISION HISTORY

| Revision | Date | Description |
|---|---|---|
| 1.0 | 03/16/2018 | Initial Release |
| 1.1 | 03/21/2018 | Revised acknowledgements |

*Originally published by 01.org