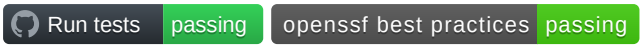
GitHub - chipsec/chipsec: Platform Security Assessment Framework

By dependabot[bot]

Archived: 2026-11-20 02:20:11 UTC



CHIPSEC is a framework for analyzing the security of PC platforms including hardware, system firmware (BIOS/UEFI), and platform components. It includes a security test suite, tools for accessing various low level interfaces, and forensic capabilities. It can be run on Windows, Linux, and UEFI shell. Instructions for installing and using CHIPSEC can be found in the manual.

NOTE: This software is for security testing purposes. Use at your own risk. Read WARNING.txt before using.

First version of CHIPSEC was released in March 2014: Announcement at CanSecWest 2014

Recent presentation on how to use CHIPSEC to find vulnerabilities in firmware, hypervisors and hardware configuration, explore low level system assets and even detect firmware implants: Exploring Your System Deeper

Release Convention

- CHIPSEC uses a major.minor.patch release version number
- Changes to the arguments or calling conventions will be held for a minor version update

Projects That Include CHIPSEC

- ArchStrike
- BlackArch Linux
- Linux UEFI Validation (LUV) (Archived)

Legacy Support (`chipsec1` branch)

If you require support for **older Intel platforms**, use the `chipsec1` branch:

- **Client Platforms:** Pre-ADL (pre-12th Gen Core)
- **Server Platforms:** Pre-SPR (pre-3rd Gen Xeon Scalable)

To switch to the legacy branch:

```
git checkout chipsec1
```

Contact Us

For any questions or suggestions please contact us at: chipsec@intel.com

Discord:

- CHIPSEC Discord Server

Twitter:

- For CHIPSEC release alerts: Follow us at CHIPSEC Release
- For general CHIPSEC info: Follow CHIPSEC

Mailing list:

- CHIPSEC discussion list on kernel.org (oe-chipsec)

For AMD related questions or suggestions please contact Gabriel Kerneis at: Gabriel.Kerneis@ssi.gouv.fr

---

Source: https://github.com/chipsec/chipsec