CVE-2018-12182

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-12182
State	PUBLIC
Assigner	secure@intel.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-27 20:29:00 UTC
Updated	2023-11-07 02:52:00 UTC
Description	Insufficient memory write check in SMM service for EDK II may allow an authenticated user to potentially enable escalation

Risk And Classification

Problem Types: CWE-441

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tianocore	Edk Ii	-	All	All	All
Application	Tianocore	Edk Ii	-	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 30 Update: edk2-20190501stable-2.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
38. SW SMI Confused Deputy SmramSaveState.c · Security Advisory	CONFIRM	edk2-docs.gitbooks.i
EDK2 CVE-2018-12182 Local Privilege Escalation Vulnerability	BID	www.securityfocus.c
[SECURITY] Fedora 30 Update: edk2-20190501stable-2.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Document Display | HPE Support Center	CONFIRM	support.hpe.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report