



CVE-2019-14562

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2019-14562
State	PUBLIC
Assigner	secure@intel.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-23 16:15:00 UTC
Updated	2022-01-01 18:10:00 UTC
Description	Integer overflow in DxelImageVerificationHandler() EDK II may allow an authenticated user to potentially enable denial of se

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Tianocore	Edk2	-	All	All	All
Application	Tianocore	Edk2	-	All	All	All

References

Reference	Source	Link	Tags
2215 – (CVE-2019-14562) DxelImageVerificationHandler integer overflow leads to endless loop	MISC	bugzilla.tianocore.org	Issue T
[SECURITY] [DLA 2645-1] edk2 security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178582](#) Debian Security Update for edk2 (DLA 2645-1)

[750627](#) OpenSUSE Security Update for ovmf (openSUSE-SU-2020:1535-1)

[750628](#) OpenSUSE Security Update for ovmf (openSUSE-SU-2020:1535-1)

© [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 registered 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](#)