



CVE-2014-0881

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-0881
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-25 20:29:00 UTC
Updated	2018-06-04 13:20:00 UTC
Description	The TPM on Integrated Management Module II (IMM2) on IBM Flex System x222 servers with firmware 1.00 through 3.56 a

Risk And Classification

Problem Types: CWE-284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	ibm	Flex System X222	-	All	All	All
Hardware	ibm	Flex System X222	-	All	All	All
Operating System	ibm	Integrated Management Module Firmware	All	All	All	All

References

Reference

IBM Support

Security Bulletin: TPM on the Integrated Management Module II (IMM2) of Flex System x222 compute node is not configured correctly (CVE-2

Security Bulletin: TPM on the Integrated Management Module II (IMM2) of Flex System x222 compute node is not configured correctly (CVE-2

CVE Program record

NVD vulnerability detail

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 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](#)