



CVE-2013-4782

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

Summary

CVE	CVE-2013-4782
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-07-08 22:55:00 UTC
Updated	2013-10-16 14:37:00 UTC
Description	The Supermicro BMC implementation allows remote attackers to bypass authentication and execute arbitrary IPMI commands.

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Supermicro	Bmc	All	All	All	All
Hardware	Supermicro	Bmc	All	All	All	All

References

Reference	Source	Link
Hacker Holes in Server Management System Allow 'Almost-Physical' Access Threat Level Wired.com	MISC	www.wired.com
93038	OSVDB	osvdb.org
[Freeipmi-devel] The Infamous Cipher Zero, I presume?	MLIST	lists.gnu.org
IPMI 2.0 Cipher Zero Authentication Bypass Scanner Rapid7	MISC	www.metasploit.com
The Infamous Cipher Zero	MISC	fish2.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 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](#)