



Hospira MedNet Use of Hard-coded Password

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2014-5405
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-03 10:59:02 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Hospira MedNet before 6.1 uses a hardcoded cleartext password to control SQL database authorization, which allows remote attackers to execute arbitrary SQL commands via the 'password' parameter.

Risk And Classification

Primary CVSS: v2.0 9 from nvd@nist.gov

AV:N/AC:L/Au:S/C:C/I:C/A:C

Problem Types: CWE-259 | CWE-200 | CWE-259 CWE-259

Version	Source	Type	Score	Severity	Vector
2.0	nvd@nist.gov	Primary	9		AV:N/AC:L/Au:S/C:C/I:C/A:C
2.0	ics-cert@hq.dhs.gov	Secondary	9		AV:N/AC:L/Au:S/C:C/I:C/A:C
2.0	CNA	CVSS	9		AV:N/AC:L/Au:S/C:C/I:C/A:C

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hospira	Mednet	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Hospira	MedNet	affected 5.8 custom	Not specified
CNA	Hospira	MedNet	unaffected 6.1	Not specified

References

Reference	Source	Link
www.cisa.gov/news-events/ics-advisories/icsa-15-090-03	ics-cert@hq.dhs.gov	www.cisa.gov
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2015/icsa-15-09...	ics-cert@hq.dhs.gov	github.com
Hospira MedNet Vulnerabilities ICS-CERT	af854a3a-2127-422b-91ae-364da2661108	ics-cert.us-cert.gov
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Billy Rios (en)

Additional Advisory Data

Solutions

CNA: Hospira has developed a new version of the MedNet software, MedNet 6.1. Hospira reports that MedNet 6.1 no longer uses hard-coded passwords, hard-coded cryptographic keys, and no longer stores passwords in clear text. Existing versions of MedNet can be upgraded to MedNet 6.1. Hospira has produced mitigation recommendations that help mitigate the vulnerability in the vulnerable version of JBoss Enterprise Application Platform software, used in the MedNet software. This has been addressed by Hospira through issuance of the following knowledge based articles: Improving Security in Hospira MedNet 5.5 (August 2014) and Improving Security in Hospira MedNet 5.8 (August 2014). For additional information about Hospira's new releases and mitigation recommendations, contact Hospira's technical support at 1-800-241-4002.

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)