



# Sensitive Data Exposure Vulnerability in e-Sushrut HMIS

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

## Summary

<b>CVE</b>	CVE-2026-42514
<b>State</b>	PUBLISHED
<b>Assigner</b>	CERT-In
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-29 09:16:24 UTC
<b>Updated</b>	2026-04-29 21:14:23 UTC
<b>Description</b>	This vulnerability exists in e-Sushrut due to exposure of OTPs in plaintext within API responses. A remote attacker could ex

## Risk And Classification

**Primary CVSS:** v4.0 8.8 HIGH from vdisclose@cert-in.org.in

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.001310000 probability, percentile 0.321490000 (date 2026-05-05)

**Problem Types:** CWE-319 | CWE-319 CWE-319 Cleartext transmission of sensitive information

Version	Source	Type	Score	Severity	Vector
4.0	vdisclose@cert-in.org.in	Secondary	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/
4.0	CNA	CVSS	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality: **High**

Integrity: **Low**

Availability: **None**

Sub Conf.: **None**

Sub Integrity: **None**

Sub Availability: **None**

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CDAC-Noida	E-Sushrut Hospital Management Information System HMIS	affected Previous versions custom	Not specified

References

Reference	Source	Link	Tags
www.cert-in.org.in/s2cMainServlet	vdisclose@cert-in.org.in	<a href="http://www.cert-in.org.in">www.cert-in.org.in</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

Vendor Comments And Credit

Discovery Credit

**CNA:** This vulnerability is reported by Harsh Verma (en)

Additional Advisory Data

Solutions

**CNA:** Contact C-DAC for upgrading e-Sushrut HMIS to latest version

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)