CVE-2026-21997

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-21997
State	PUBLISHED
Assigner	oracle
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 21:16:24 UTC
Updated	2026-04-22 21:24:26 UTC
Description	Vulnerability in the Oracle Life Sciences Empirica Signal product of Oracle Life Science Applications (component: Common

Risk And Classification

Primary CVSS: v3.1 8.5 HIGH from secalert_us@oracle.com

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N

EPSS: 0.000270000 probability, percentile 0.077630000 (date 2026-04-22)

Problem Types: CWE-284 | Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Life Sciences Empirica Signal. While the vulnerability is in Oracle Life Sciences Empirica Signal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Life Sciences Empirica Signal accessible data as well as unauthorized read access to a subset of Oracle Life Sciences Empirica Signal accessible data. | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	secalert_us@oracle.com	Secondary	8.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N
3.1	CNA	DECLARED	8.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Oracle Corporation	Oracle Life Sciences Empirica Signal	affected 9.2.1 9.2.3 custom	Not specified

References

Reference	Source	Link	Tags
www.oracle.com/security-alerts/cpuapr2026.html	secalert_us@oracle.com	www.oracle.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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