



Gainsight Assist plugin information disclosure

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

Summary

CVE	CVE-2026-31381
State	PUBLISHED
Assigner	rapid7
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-20 14:16:14 UTC
Updated	2026-04-16 15:16:53 UTC
Description	An attacker can extract user email addresses (PII) exposed in base64 encoding via the state parameter in the OAuth callba

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from cve@rapid7.com

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

EPSS: 0.000130000 probability, percentile 0.023680000 (date 2026-04-21)

Problem Types: CWE-598 | NVD-CWE-noinfo | CWE-598 CWE-598 Use of GET request method with sensitive query strings

Version	Source	Type	Score	Severity	Vector
3.1	cve@rapid7.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gainsight	Assist	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Gainsight	Gainsight Assist	unknown semver	Not specified

References

Reference	Source	Link
communities.gainsight.com/community-news-2/recent-gainsight-assist-plugin-remediations-...	cve@rapid7.com	communities.gainsight.com
www.rapid7.com/blog/post/ve-cve-2026-31381-cve-2026-31382-gainsight-assist-i...	cve@rapid7.com	www.rapid7.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Christopher O'Boyle, Cybersecurity Advisor at Rapid7 (en)

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