CVE-2014-0999

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

Summary

CVE	CVE-2014-0999
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-02 14:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Sendio before 7.2.4 includes the session identifier in URLs in emails, which allows remote attackers to obtain sensitive infor

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-200 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sendio	Sendio	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.se
Full Disclosure: [CORE-2015-0010] - Sendio ESP Information Disclosure Vulnerability	af854a3a-2127-422b-91ae-364da2661108	seclists.
Software Release History | Email Security and Efficiency – Sendio	af854a3a-2127-422b-91ae-364da2661108	www.se
Sendio ESP Information Disclosure ≈ Packet Storm	af854a3a-2127-422b-91ae-364da2661108	packets
Sendio ESP - Information Disclosure	af854a3a-2127-422b-91ae-364da2661108	www.ex
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

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