



CVE-2015-0932

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

Summary

CVE	CVE-2015-0932
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-05 01:59:00 UTC
Updated	2015-04-15 17:02:00 UTC
Description	The ANTLabs InnGate firmware on IG 3100, IG 3101, InnGate 3.00 E, InnGate 3.01 E, InnGate 3.02 E, InnGate 3.10 E, Inn

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Antlabs	Inngate Ig 3.00 E	All	All	All	All
Hardware	Antlabs	Inngate Ig 3.00 E	All	All	All	All
Hardware	Antlabs	Inngate Ig 3.01 E	All	All	All	All
Hardware	Antlabs	Inngate Ig 3.01 E	All	All	All	All
Hardware	Antlabs	Inngate Ig 3.02 E	All	All	All	All
Hardware	Antlabs	Inngate Ig 3.02 E	All	All	All	All
Hardware	Antlabs	Inngate Ig 3.10 E	All	All	All	All
Hardware	Antlabs	Inngate Ig 3.10 E	All	All	All	All
Hardware	Antlabs	Inngate Ig 3.10 G	All	All	All	All
Hardware	Antlabs	Inngate Ig 3.10 G	All	All	All	All
Hardware	Antlabs	Inngate Ig 3100	All	All	All	All
Hardware	Antlabs	Inngate Ig 3100	All	All	All	All
Hardware	Antlabs	Inngate Ig 3101	All	All	All	All
Hardware	Antlabs	Inngate Ig 3101	All	All	All	All

References

Reference	Source	Link
-----------	--------	------

ANTlabs: Connectivity Made Easy	CONFIRM	www.antlabs.com
Vulnerability Note VU#930956 - Multiple ANTLabs InnGate models allow unauthenticated read/write to filesystem	CERT-VN	www.kb.cert.org
Big Vulnerability in Hotel Wi-Fi Router Puts Guests at Risk WIRED	MISC	www.wired.com
Vulnerability: CVE-2015-0932	MISC	blog.cylance.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov



No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://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