



# CVE-2011-3997

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

## Summary

<b>CVE</b>	CVE-2011-3997
<b>State</b>	PUBLIC
<b>Assigner</b>	vultures@jpcert.or.jp
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-11-09 20:55:00 UTC
<b>Updated</b>	2011-11-16 05:00:00 UTC
<b>Description</b>	Opengear console servers with firmware before 2.2.1 allow remote attackers to bypass authentication, and modify settings

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Opengear	Acm5000 Console Server	All	All	All	All
Hardware	Opengear	Acm5000 Console Server	All	All	All	All
Hardware	Opengear	Cm4000 Console Server	All	All	All	All
Hardware	Opengear	Cm4000 Console Server	All	All	All	All
Hardware	Opengear	Im4004-5 Console Server	All	All	All	All
Hardware	Opengear	Im4004-5 Console Server	All	All	All	All
Hardware	Opengear	Im4200 Console Server	All	All	All	All
Hardware	Opengear	Im4200 Console Server	All	All	All	All
Hardware	Opengear	Img4000 Console Server	All	All	All	All
Hardware	Opengear	Img4000 Console Server	All	All	All	All
Hardware	Opengear	Kcs6000 Rackside Console Server	All	All	All	All
Hardware	Opengear	Kcs6000 Rackside Console Server	All	All	All	All
Application	Opengear	Opengear Console Server Firmware	2.0.4	All	All	All
Application	Opengear	Opengear Console Server Firmware	2.0.4u1	All	All	All
Application	Opengear	Opengear Console Server Firmware	2.0.6	All	All	All
Application	Opengear	Opengear Console Server Firmware	2.0.8	All	All	All
Application	Opengear	Opengear Console Server Firmware	2.0.9	All	All	All

Application	<a href="#">Opengear</a>	<a href="#">Opengear Console Server Firmware</a>	2.1.0	All	All	All
Application	<a href="#">Opengear</a>	<a href="#">Opengear Console Server Firmware</a>	2.1.0u1	All	All	All
Application	<a href="#">Opengear</a>	<a href="#">Opengear Console Server Firmware</a>	2.0.4	All	All	All
Application	<a href="#">Opengear</a>	<a href="#">Opengear Console Server Firmware</a>	2.0.4u1	All	All	All
Application	<a href="#">Opengear</a>	<a href="#">Opengear Console Server Firmware</a>	2.0.6	All	All	All
Application	<a href="#">Opengear</a>	<a href="#">Opengear Console Server Firmware</a>	2.0.8	All	All	All
Application	<a href="#">Opengear</a>	<a href="#">Opengear Console Server Firmware</a>	2.0.9	All	All	All
Application	<a href="#">Opengear</a>	<a href="#">Opengear Console Server Firmware</a>	2.1.0	All	All	All
Application	<a href="#">Opengear</a>	<a href="#">Opengear Console Server Firmware</a>	2.1.0u1	All	All	All
Application	<a href="#">Opengear</a>	<a href="#">Opengear Console Server Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Tags
JVNDB-2011-000096	JVNDB	<a href="http://jvndb.jvn.jp">jvndb.jvn.jp</a>	
JVN#71349007: Opengear console servers vulnerable to authentication bypass	JVN	<a href="http://jvn.jp">jvn.jp</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

No vendor comments have been submitted for this CVE.

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](#).

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