



CVE-2005-0865

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

Summary

CVE	CVE-2005-0865
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2008-09-05 20:47:00 UTC
Description	Samsung ADSL Modem SMDK8947v1.2 uses default passwords for the (1) root, (2) admin, or (3) user users, which allows

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Securecomputing	Samsung Adsl Modem	smdk8947v1.2	All	All	All
Hardware	Securecomputing	Samsung Adsl Modem	smdk8947v1.2	All	All	All

References

Reference

exploitlabs.com/files/advisories/EXPL-A-2005-002-samsung-adsl.txt

[SecurityTracker.com Archives - Samsung ADSL Router Discloses Files to Remote Users and May Grant Root Access Via Common Default P](#)

[Samsung DSL Modem Multiple Remote Vulnerabilities](#)

zone-h.org/en/advisories/read/id=7339

[CVE Program record](#)

[NVD vulnerability detail](#)

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](#)