



CVE-2002-2380

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

Summary

CVE	CVE-2002-2380
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-12-31 05:00:00 UTC
Updated	2008-09-05 20:33:00 UTC
Description	NetDSL ADSL Modem 800 with Microsoft Network firmware 5.5.11 allows remote attackers to gain access to configuration

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Arescom	Netdsl	800	All	All	All
Hardware	Arescom	Netdsl	800	All	All	All
Application	Microsoft	Network Firmware	5.5.11	All	All	All
Application	Microsoft	Network Firmware	5.5.11	All	All	All

References

Reference
RUS-CERT - Requested Page not found
Arescom NetDSL-800 Firmware Undocumented Username/Password Weakness
ISS X-Force Database: netdsl-msn-default-account (10498): NetDSL-800 included with MSN DSL services provides a default username and p
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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)