



CVE-2010-2967

Published on: 08/04/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:09 PM UTC

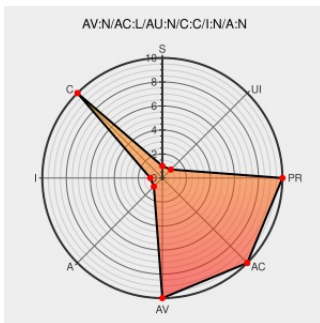
CVE-2010-2967

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Vxworks](#) from [Windriver](#) contain the following vulnerability:

The loginDefaultEncrypt algorithm in loginLib in Wind River VxWorks before 6.9 does not properly support a large set of distinct possible passwords, which makes it easier for remote attackers to obtain access via a (1) telnet, (2) rlogin, or (3) FTP session.

CVE-2010-2967 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

**Access
Vector**

NETWORK

**Access
Complexity**

LOW

Authentication

NONE

**Confidentiality
Impact**

COMPLETE

**Integrity
Impact**

NONE

**Availability
Impact**

NONE

CVE References

Description

Tags

Link

Metasploit: Shiny Old VxWorks Vulnerabilities

[blog.metasploit.com](#)
[text/html](#)

[MISC blog.metasploit.com/2010/08/vxworks-vulnerabilities.html](#)

US-CERT Vulnerability Note VU#840249

[US Government Resource](#)
[www.kb.cert.org](#)
[text/html](#)

[CERT-VN VU#840249](#)

Wind River

[support.windriver.com](#)
[text/html](#)

[CONFIRM support.windriver.com/olsPortal/faces/maintenance/downloadDetails.jspx?contentId=033709](#)

Wind River Systems, Inc. Information for VU#840249

[www.kb.cert.org](#)
[text/html](#)

[CONFIRM www.kb.cert.org/vuls/id/MAPG-863QH9](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further,

are more appropriate for your purposes. CVEreport does not necessarily endorse the items expressed, or content that are listed presented on these sites. CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Windriver	Vxworks	5	All	All	All
Operating System	Windriver	Vxworks	5.5	All	All	All
Operating System	Windriver	Vxworks	6	All	All	All
Operating System	Windriver	Vxworks	6.4	All	All	All
Operating System	Windriver	Vxworks	5	All	All	All
Operating System	Windriver	Vxworks	5.5	All	All	All
Operating System	Windriver	Vxworks	6	All	All	All
Operating System	Windriver	Vxworks	6.4	All	All	All
Operating System	Windriver	Vxworks	All	All	All	All
cpe:2.3:o:windriver:vxworks:5:*****:*						
cpe:2.3:o:windriver:vxworks:5.5:*****:*						
cpe:2.3:o:windriver:vxworks:6:*****:*						
cpe:2.3:o:windriver:vxworks:6.4:*****:*						
cpe:2.3:o:windriver:vxworks:5:*****:*						
cpe:2.3:o:windriver:vxworks:5.5:*****:*						
cpe:2.3:o:windriver:vxworks:6:*****:*						
cpe:2.3:o:windriver:vxworks:6.4:*****:*						
cpe:2.3:o:windriver:vxworks:*****:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)