



CVE-2003-1391

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-1391

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Cryptobuddy](#) from [Research Triangle Software](#) contain the following vulnerability:

RTS CryptoBuddy 1.0 and 1.2 uses a weak encryption algorithm for the passphrase and generates predictable keys, which makes it easier for attackers to guess the passphrase.

CVE-2003-1391 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
[text/html](#)

[XF cryptobuddy-password-dictionary\(11298\)](#)

SecurityFocus

[www.securityfocus.com](https://www.securityfocus.com/text/html)
[text/html](#)

[BUGTRAQ 20030210 RTS CryptoBuddy Multiple Encryption Implementation Vulnerabilities](#)

CryptoBuddy Predictable Encrypted
Passphrase Weakness

[cve.report \(archive\)](#)
[text/html](#)

[BID 6810](#)

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, 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
Application	Research Triangle Software	Cryptobuddy	1.0	All	All	All
Application	Research Triangle Software	Cryptobuddy	1.2	All	All	All
Application	Research Triangle Software	Cryptobuddy	1.0	All	All	All
Application	Research Triangle Software	Cryptobuddy	1.2	All	All	All
cpe:2.3:a:research_triangle_software:cryptobuddy:1.0:*:*:*:*:*:						
cpe:2.3:a:research_triangle_software:cryptobuddy:1.2:*:*:*:*:*:						
cpe:2.3:a:research_triangle_software:cryptobuddy:1.0:*:*:*:*:*:						
cpe:2.3:a:research_triangle_software:cryptobuddy:1.2:*:*:*:*:*:						

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