



CVE-2008-0580

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

Summary

CVE	CVE-2008-0580
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-02-05 03:00:00 UTC
Updated	2018-10-15 22:01:00 UTC
Description	Geert Moernaut LRunasE and Supercrypt use an encryption key composed of an SHA1 hash of a fixed string embedded in

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Geert Moernaut	Lsrunase	All	All	All	All
Application	Geert Moernaut	Lsrunase	All	All	All	All
Application	Geert Moernaut	Supercrypt	All	All	All	All
Application	Geert Moernaut	Supercrypt	All	All	All	All

References

Reference	Source	Link	Tags
Insecure Use of RC4 in LRunasE and Supercrypt (CVE-2007-6340) - CXSecurity.com	SREASON	securityreason.com	
SecurityFocus	BUGTRAQ	www.securityfocus.com	
LRunase and Supercrypt RC4 Weak Encryption Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, authoritative

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](#)