



CVE-2008-1705

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

Summary

CVE	CVE-2008-1705
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-04-09 19:05:00 UTC
Updated	2018-10-11 20:36:00 UTC
Description	Format string vulnerability in the logging function in IBM solidDB 06.00.1018 and earlier allows remote attackers to execute

Risk And Classification

Problem Types: CWE-134

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Soliddb	06.00.1018	All	All	All
Application	Ibm	Soliddb	06.00.1018	All	All	All

References

Reference
Direct Link
IBM solidDB Multiple Vulnerabilities - Advisories - Secunia
Webmail - OVH
SecurityFocus
IBM X-Force Exchange
IBM solidDB Format String Vulnerability and Multiple Denial of Service Vulnerabilities
SecurityTracker.com Archives - IBM solidDB Format String and Memory Errors Let Remote Users Execute Arbitrary Code or Deny Service
alugi.altervista.org/adv/soliduro-adv.txt
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](#)