



CVE-2001-1319

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

Summary

CVE	CVE-2001-1319
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-07-16 04:00:00 UTC
Updated	2020-04-09 13:42:00 UTC
Description	Microsoft Exchange 5.5 2000 allows remote attackers to cause a denial of service (hang) via exceptional BER encodings fo

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Exchange Server	2000	-	All	All
Application	Microsoft	Exchange Server	5.5	-	All	All
Application	Microsoft	Exchange Server	2000	-	All	All
Application	Microsoft	Exchange Server	5.5	-	All	All

References

Reference	Source
L-116	CIAC
IBM X-Force Exchange	XF
www.ee.oulu.fi/research/ouspg/protos/testing/c06/ldapv3	MISC
CERT Advisory CA-2001-18 Multiple Vulnerabilities in Several Implementations of the Lightweight Directory Access Protocol (LDAP)	CERT
Microsoft Information for VU#763400	CONF
Microsoft Exchange 5.5 LDAP Denial of Service Vulnerabilities	BID
CERT/CC Vulnerability Note VU#763400	CERT
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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](#)