CVE-2003-0805

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2003-0805
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-10-06 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple buffer overflows in UMN gopher daemon (gopherd) 2.x and 3.x before 3.0.6 allows attackers to execute arbitrary cc

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	University Of Minnesota	Gopherd	2.0.3	All	All	All

Application	University Of Minnesota	Gopherd	2.0.4	All	All	All
Application	University Of Minnesota	Gopherd	2.3	All	All	All
Application	University Of Minnesota	Gopherd	2.3.1	All	All	All
Application	University Of Minnesota	Gopherd	3.0.0	All	All	All
Application	University Of Minnesota	Gopherd	3.0.1	All	All	All
Application	University Of Minnesota	Gopherd	3.0.2	All	All	All
Application	University Of Minnesota	Gopherd	3.0.3	All	All	All
Application	University Of Minnesota	Gopherd	3.0.4	All	All	All
Application	University Of Minnesota	Gopherd	3.0.5	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link	Tag
'FW: [gopher] UMN Gopher 3.0.6 released' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info	
'UMN gopherd[2.x.x/3.x.x]: ftp gateway, and GSisText() buffer' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info	
Debian -- Security Information -- DSA-387-1 gopher	af854a3a-2127-422b-91ae-364da2661108	www.debian.org	Patc
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.