CVE-2009-0241

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

Summary

CVE	CVE-2009-0241
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-21 11:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Stack-based buffer overflow in the process_path function in gmetad/server.c in Ganglia 3.1.1 allows remote attackers to cau

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: CWE-119 | 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	Ganglia	Ganglia	3.1.1	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Ganglia "process_path()" Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b-9
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:011	af854a3a-2127-422b-9
[Ganglia-developers] patches for: [Sec] Gmetad server BoF and network ov	af854a3a-2127-422b-9
Gentoo Linux Documentation -- Ganglia: Execution of arbitrary code	af854a3a-2127-422b-9
Gentoo update for ganglia - Secunia.com	af854a3a-2127-422b-9
Bug 223 - CVE-2009-0241: Buffer overflow in gmetad's interactive port	af854a3a-2127-422b-9
Ganglia gmetad 'process_path()' Remote Stack Buffer Overflow Vulnerability	af854a3a-2127-422b-9
SUSE Update for Multiple Packages - Advisories - Community	af854a3a-2127-422b-9
[Ganglia-developers] patches for: [Sec] Gmetad server BoF and network ov	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-01-23	Tomas Hoger	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com

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