CVE-2004-1752

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

Summary

CVE	CVE-2004-1752
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-08-24 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Stack-based buffer overflow in Gaucho 1.4 Build 145 allows remote attackers to execute arbitrary code via a POP3 email w

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	Nakedsoft	Gaucho	1.4_build_145	All	All	All

Vendor Declared Affected Products

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

References

Reference
Secunia - Advisories - Gaucho "Content-Type:" Header Processing Buffer Overflow Vulnerability
Gaucho Buffer Overflow in Processing Mail Headers Via POP3 Lets Remote Servers Execute Arbitrary Code - SecurityTracker
SIG^2 G-TEC - Gaucho 1.4 Email Client has Buffer Overflow Vulnerability when Receiving Email Headers with Abnormally Long Content-Type
NakedSoft Gaucho POP3 Email Header Buffer Overflow Vulnerability
IBM X-Force Exchange
'Gaucho v1.4 Build 145 Buffer Overflow' - MARC
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.