CVE-2002-0548

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

Summary

CVE	CVE-2002-0548
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-07-03 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Anthill allows remote attackers to bypass authentication and file bug reports by directly accessing the postbug.php program

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	Anthill	Anthill	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Neohapsis Archives - Bugtraq - Anthill login and JavaScript vulnerabilities - From ulfhupdate.uu.se	af854a3a-2127-422b-91ae-364da266
ISS X-Force Database: anthill-postbug-auth-bypass (8771): Anthill postbug.php authentication bypass	af854a3a-2127-422b-91ae-364da266
Anthill postbug.php Authentication Bypass Vulnerability	af854a3a-2127-422b-91ae-364da266
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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