CVE-2006-6701

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

Summary

CVE	CVE-2006-6701
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-12-23 01:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Cross-site request forgery (CSRF) vulnerability in util.pl in @Mail WebMail 4.51, and util.php in 5.x before 5.03, allows remo

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-352 | 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	Atmail	Atmail Webmail	3.0	All	All	All

Application	Atmail	Atmail Webmail	4.0	All	All	All
Application	Atmail	Atmail Webmail	4.51	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Netragard - Penetration Testing, Red Teaming & App Testing Company	af854a3a-2127-422b-9
@Mail "util.php" Cross-Site Request Forgery - Advisories - Secunia	af854a3a-2127-422b-9
SecurityFocus	af854a3a-2127-422b-9
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-9
@Mail Input Validation Holes Permit Cross-Site Scripting and Cross-Site Request Forgery Attacks - SecurityTracker	af854a3a-2127-422b-9
@Mail Changelog - Latest release	af854a3a-2127-422b-9
IBM X-Force Exchange	af854a3a-2127-422b-9
@Mail Webmail Two Vulnerabilities - Advisories - Secunia	af854a3a-2127-422b-9
archives.neohapsis.com/archives/fulldisclosure/2007-01/0512.html	af854a3a-2127-422b-9
Netragard - Penetration Testing, Red Teaming & App Testing Company	af854a3a-2127-422b-9
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.