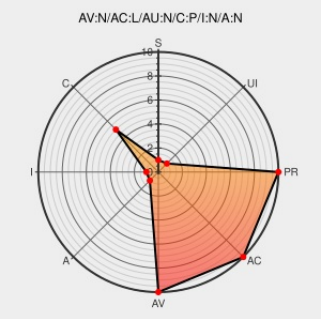
CVE-2004-1549

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1549

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Activepost Standard from Onnuri Infotek contain the following vulnerability:

The conference menu in ActivePost Standard 3.1 sends passwords of password-protected rooms in cleartext, which could allow remote attackers to gain sensitive information by sniffing the network connection.

CVE-2004-1549 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
	aluigi.altervista.org text/plain	MISC aluigi.altervista.org/adv/actp-adv.txt
SecurityTracker.com Archives - ActivePost Lets Remote Users Upload Arbitrary Files, Detemine Passwords, and Crash the System, and D	securitytracker.com text/html	SECTRACK 1011406
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF activepost-plaintext-password(17486)
ActivePost Messenger Multiple Remote Vulnerabilities	cve.report (archive) text/html	BID 11244
'Multiple vulnerabilities in ActivePost Standard 3.1' - MARC	marc.info text/html	BUGTRAQ 20040923 Multiple vulnerabilities in ActivePost Standard 3.1

Secunia - Advisories - ActivePost Standard Multiple Vulnerabilities

Vendor Advisory
web.archive.org
text/html

SECUNIA 12642

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Onnuri Infotek	Activepost Standard	3.1	All	All	All
Application	Onnuri Infotek	Activepost Standard	3.1	All	All	All

cpe:2.3:a:onnuri_infotek:activepost_standard:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:onnuri_infotek:activepost_standard:3.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→