CVE-2005-4270

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

Summary

CVE	CVE-2005-4270
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-12-15 20:11:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in Watchfire AppScan QA 5.0.609 and 5.0.134 allows remote web servers to execute arbitrary code via an H

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	Watchfire	Appscan Qa	5.0.134	All	All	All

Application	Watchfire	Appscan Qa	5.0.609	All	All	All

Vendor Declared Affected Products

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

References

Reference
SecurityFocus
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
www.cybsec.com/vuln/CYBSEC_Security_Advisory_AppScanQA_RemoteCodeExec.pdf
Secunia - Advisories - AppScan QA HTTP Response Handling Buffer Overflow Vulnerability
CXSecurity - IDS
Watchfire AppScan Buffer Overflow in Processing HTTP 401 Response Messages Lets Remote Users Execute Arbitrary Code - SecurityTrack
Watchfire AppScan QA Remote Buffer Overflow Vulnerability
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.