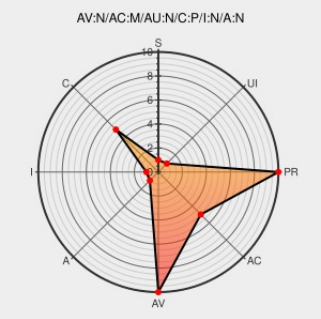
CVE-2007-3571

Published on: 07/05/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:33 PM UTC

CVE-2007-3571

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



Certain versions of Groupwise from Novell contain the following vulnerability:

The Apache Web Server as used in Novell NetWare 6.5 and GroupWise allows remote attackers to obtain sensitive information via a certain directive to Apache that causes the HTTP-Header response to be modified, which may reveal the server's internal IP address.

CVE-2007-3571 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF novell-httpheader-information-disclosure(35365)
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 45742
No Description Provided	secure-support.novell.com Inactive Link Not Archived	CONFIRM secure-support.novell.com/KanisaPlatform/Publishing/370/3555327_f.SAL_Public.html
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2007-2388

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Novell	Groupwise	6.0	All	All	All
Application	Novell	Groupwise	6.0	sp1	All	All
Application	Novell	Groupwise	6.0	sp2	All	All
Application	Novell	Groupwise	6.0	sp3	All	All
Application	Novell	Groupwise	6.0	sp4	All	All
Application	Novell	Groupwise	6.0.1	sp1	All	All
Application	Novell	Groupwise	6.5	All	All	All
Application	Novell	Groupwise	6.5	sp1	All	All
Application	Novell	Groupwise	6.5	sp2	All	All
Application	Novell	Groupwise	6.5	sp3	All	All
Application	Novell	Groupwise	6.5	sp4	All	All
Application	Novell	Groupwise	6.5	sp5	All	All
Application	Novell	Groupwise	6.5	sp6	All	All
Application	Novell	Groupwise	6.5.2	All	All	All
Application	Novell	Groupwise	6.5.3	All	All	All
Application	Novell	Groupwise	6.5.4	All	All	All
Application	Novell	Groupwise	7.0	All	All	All
Application	Novell	Groupwise	7.0	sp1	All	All
Application	Novell	Groupwise	6.0	All	All	All
Application	Novell	Groupwise	6.0	sp1	All	All
Application	Novell	Groupwise	6.0	sp2	All	All
Application	Novell	Groupwise	6.0	sp3	All	All
Application	Novell	Groupwise	6.0	sp4	All	All
Application	Novell	Groupwise	6.0.1	sp1	All	All
Application	Novell	Groupwise	6.5	All	All	All
Application	Novell	Groupwise	6.5	sp1	All	All
Application	Novell	Groupwise	6.5	sp2	All	All
Application	Novell	Groupwise	6.5	sp3	All	All
Application	Novell	Groupwise	6.5	sp4	All	All

Application	Novell	Groupwise	6.5	sp5	All	All
Application	Novell	Groupwise	6.5	sp6	All	All
Application	Novell	Groupwise	6.5.2	All	All	All
Application	Novell	Groupwise	6.5.3	All	All	All
Application	Novell	Groupwise	6.5.4	All	All	All
Application	Novell	Groupwise	7.0	All	All	All
Application	Novell	Groupwise	7.0	sp1	All	All
Operating System	Novell	Netware	6.5	All	All	All
Operating System	Novell	Netware	6.5	All	All	All

- cpe:2.3:a:novell:groupwise:6.0:*:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.0:sp1:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.0:sp2:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.0:sp3:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.0:sp4:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.0.1:sp1:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.5:*:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.5:sp1:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.5:sp2:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.5:sp3:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.5:sp4:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.5:sp5:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.5:sp6:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.5.2:*:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.5.3:*:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.5.4:*:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:7.0:*:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:7.0:sp1:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.0:*:*:*:*:*:*:*:
- cpe:2.3:a:novell:groupwise:6.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.0.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.5:*:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.5:sp1:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.5:sp2:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.5:sp3:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.5:sp4:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.5:sp5:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.5:sp6:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:6.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:novell:groupwise:7.0:sp1:*:*:*:*:*:*:

cpe:2.3:o:novell:netware:6.5:*:*:*:*:*:*:*:

cpe:2.3:o:novell:netware:6.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→