

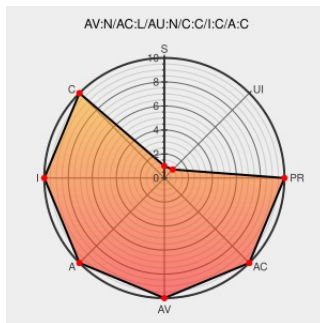


# CVE-2010-4714

Published on: 01/31/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:00 PM UTC

## CVE-2010-4714

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Groupwise](#) from [Novell](#) contain the following vulnerability:

Multiple stack-based buffer overflows in Novell GroupWise before 8.02HP allow remote attackers to execute arbitrary code via a long HTTP Host header to (1) gwpoa.exe in the Post Office Agent, (2) gwmata.exe in the Message Transfer Agent, (3) gwia.exe in the Internet Agent, (4) the WebAccess Agent, or (5) the Monitor Agent.

CVE-2010-4714 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access  
Vector

**NETWORK**

Access  
Complexity

**LOW**

Authentication

**NONE**

Confidentiality  
Impact

**COMPLETE**

Integrity  
Impact

**COMPLETE**

Availability  
Impact

**COMPLETE**

## CVE References

Description

Tags

Link

GroupWise 8.0.2 Hot Patch Ships! | Facebook

[www.facebook.com](#)  
[text/html](#)

[CONFIRM](#) [www.facebook.com/note.php?note\\_id=477865030928](#)

Zero Day Initiative

[zerodayinitiative.com](#)  
[text/html](#)

[MISC](#) [zerodayinitiative.com/advisories/ZDI-10-247/](#)

No Description Provided

[Vendor Advisory](#)  
[www.novell.com](#)  
[text/html](#)

[ot CONFIRM](#) [www.novell.com/support/viewContent.do?externalId=7007159&sliceId=1](#)

Access Denied

[bugzilla.novell.com](#)  
[text/html](#)

[CONFIRM](#) [bugzilla.novell.com/show\\_bug.cgi?id=627942](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

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](mailto: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 | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 4.1     | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 4.1a    | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 5.0     | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 5.1     | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 5.2     | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 5.5     | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 5.5     | All    | enhancement_pack | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 5.57e   | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.0     | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.0     | sp1    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.0     | sp5    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.0.1   | sp1    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.5     | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.5     | sp1    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.5     | sp2    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.5     | sp3    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.5     | sp4    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.5     | sp5    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.5     | sp6    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.5.2   | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.5.3   | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.5.4   | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.5.6   | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 6.5.7   | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 7.0     | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 7.0.1   | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 7.0.2   | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 7.0.3   | All    | All              | All      |
| Application | <a href="#">Novell</a> | <a href="#">Groupwise</a> | 7.0.4   | All    | All              | All      |



|                                                          |
|----------------------------------------------------------|
| cpe:2.3:a:novell:groupwise:4.1a:*****:*                  |
| cpe:2.3:a:novell:groupwise:5.0:*****:*                   |
| cpe:2.3:a:novell:groupwise:5.1:*****:*                   |
| cpe:2.3:a:novell:groupwise:5.2:*****:*                   |
| cpe:2.3:a:novell:groupwise:5.5:*****:*                   |
| cpe:2.3:a:novell:groupwise:5.5:*enhancement_pack:*****:* |
| cpe:2.3:a:novell:groupwise:5.57e:*****:*                 |
| 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:sp5:*****:*               |
| 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:6.5.6:*****:*                 |
| cpe:2.3:a:novell:groupwise:6.5.7:*****:*                 |
| cpe:2.3:a:novell:groupwise:7.0:*****:*                   |
| cpe:2.3:a:novell:groupwise:7.0.1:*****:*                 |
| cpe:2.3:a:novell:groupwise:7.0.2:*****:*                 |
| cpe:2.3:a:novell:groupwise:7.0.3:*****:*                 |
| cpe:2.3:a:novell:groupwise:7.0.4:*****:*                 |
| cpe:2.3:a:novell:groupwise:8.0:*****:*                   |

|                                                            |
|------------------------------------------------------------|
| cpe:2.3:a:novell:groupwise:8.0:*:*:*:*:*:                  |
| cpe:2.3:a:novell:groupwise:8.0.1:*:*:*:*:*:                |
| cpe:2.3:a:novell:groupwise:4.1:*:*:*:*:*:                  |
| cpe:2.3:a:novell:groupwise:4.1a:*:*:*:*:*:                 |
| cpe:2.3:a:novell:groupwise:5.0:*:*:*:*:*:                  |
| cpe:2.3:a:novell:groupwise:5.1:*:*:*:*:*:                  |
| cpe:2.3:a:novell:groupwise:5.2:*:*:*:*:*:                  |
| cpe:2.3:a:novell:groupwise:5.5:*:*:*:*:*:                  |
| cpe:2.3:a:novell:groupwise:5.5:*:enhancement_pack:*:*:*:*: |
| cpe:2.3:a:novell:groupwise:5.57e:*:*:*:*:*:                |
| 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:sp5:*:*:*:*:*:              |
| 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:6.5.6:*:*:*:*:*:                |
| cpe:2.3:a:novell:groupwise:6.5.7:*:*:*:*:*:                |
| cpe:2.3:a:novell:groupwise:7.0:*:*:*:*:*:                  |
| cpe:2.3:a:novell:groupwise:7.0.1:*:*:*:*:*:                |
| cpe:2.3:a:novell:groupwise:7.0.2:*:*:*:*:*:                |

|                                         |
|-----------------------------------------|
| cpe:2.3:a:novell:groupwise:7.0.3:*****: |
| cpe:2.3:a:novell:groupwise:7.0.4:*****: |
| cpe:2.3:a:novell:groupwise:8.0:*****:   |
| cpe:2.3:a:novell:groupwise:8.0.1:*****: |
| cpe:2.3:a:novell:groupwise:*****:       |

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →