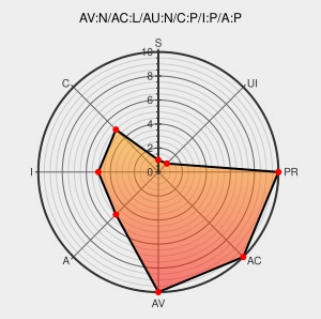
CVE-2004-2203

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

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2203

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



Certain versions of Ansel from Ansel contain the following vulnerability:

Ansel 1.2 through 2.0 uses insecure default permissions, which allows remote attackers to gain access to web readable directories.

CVE-2004-2203 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Federico David Sacerdoti Ansel Insecure Default Permissions Vulnerability	Patch, cve.report (archive), text/html	BID 11420
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF ansell-gain-access(17767)
No Description Provided	Patch, www.osvdb.org, Inactive Link, Not Archived	OSVDB 10898
SecurityTracker.com Archives - Ansel May Disclose Photo Album Directories to Remote Users	Patch, securitytracker.com, text/html	SECTRACK 1011775

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ansel	Ansel	1.2	All	All	All
Application	Ansel	Ansel	1.3	All	All	All
Application	Ansel	Ansel	1.4	All	All	All
Application	Ansel	Ansel	2.0	All	All	All
Application	Ansel	Ansel	1.2	All	All	All
Application	Ansel	Ansel	1.3	All	All	All
Application	Ansel	Ansel	1.4	All	All	All
Application	Ansel	Ansel	2.0	All	All	All

cpe:2.3:a:ansel:ansel:1.2:*:*:*:*:*:*:*

cpe:2.3:a:ansel:ansel:1.3:*:*:*:*:*:*:*

cpe:2.3:a:ansel:ansel:1.4:*:*:*:*:*:*:*

cpe:2.3:a:ansel:ansel:2.0:*:*:*:*:*:*:*

cpe:2.3:a:ansel:ansel:1.2:*:*:*:*:*:*:*

cpe:2.3:a:ansel:ansel:1.3:*:*:*:*:*:*:*

cpe:2.3:a:ansel:ansel:1.4:*:*:*:*:*:*:*

cpe:2.3:a:ansel:ansel:2.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→