

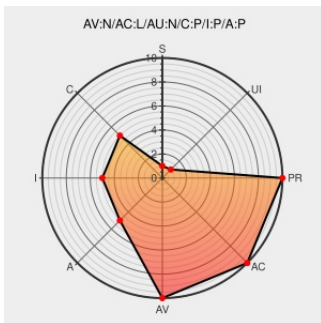


CVE-2004-2266

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

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

CVE-2004-2266

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

Certain versions of [Ansel](#) from [Ansel](#) contain the following vulnerability:
SQL injection vulnerability in Ansel 2.1 and earlier allows remote attackers to modify SQL statements via the image parameter.

CVE-2004-2266 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Secunia - Advisories - Ansel "image" SQL Injection and Script Insertion Vulnerabilities

[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[X](#) [SECUNIA 12856](#)

Ansel Multiple Input Validation Vulnerabilities

[Patch](#)
[cve.report \(archive\)](#)
[text/html](#)

[🌐](#) [BID 11824](#)

SecurityTracker.com Archives - Ansel Input Validation Hole in 'image' Parameter Lets Remote Users Inject SQL Commands and Conduct Cross-Site Scripting Attacks

[Patch](#)
[securitytracker.com](#)
[text/html](#)

[🌐](#) [SECTRAK 1012434](#)

No Description Provided

[Patch](#)
[www.osvdb.org](#)

[🌐](#) [OSVDB 12236](#)

[Inactive Link](#) [Not Archived](#)

About Secunia Research | Flexera

Patch

Vendor Advisory

secunia.com

Depreciated Link

text/plain

X MISC
secunia.com/secunia_research/2004-17/advisory/

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	1.0	All	All	All
Application	Ansel	Ansel	1.1	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
Application	Ansel	Ansel	2.1	All	All	All
Application	Ansel	Ansel	1.0	All	All	All
Application	Ansel	Ansel	1.1	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
Application	Ansel	Ansel	2.1	All	All	All

```
cpe:2.3:a:ansel:ansel:1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:ansel:ansel:1.1:*:*:*:*:*:*:
```

```
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:2.1:*:*:*:*:*:

cpe:2.3:a:ansel:ansel:1.0:*:*:*:*:*:	
cpe:2.3:a:ansel:ansel:1.1:*:*:*:*:*:	
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:2.1:*:*:*:*:*:	
No vendor comments have been submitted for this CVE	
← Previous ID	Next ID→