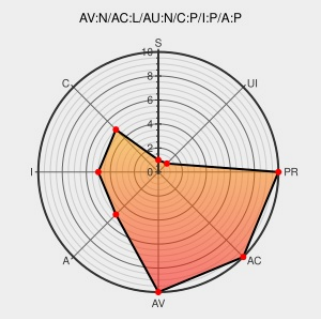
# CVE-2004-2173

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

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

## CVE-2004-2173

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




Certain versions of Productcart from Early Impact contain the following vulnerability:

SQL injection vulnerability in advSearch_h.asp in EarlyImpact ProductCart allows remote attackers to execute arbitrary SQL commands via the priceUntil parameter.

CVE-2004-2173 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 |
|---|---|---|
| SecurityFocus | Exploit, www.securityfocus.com, text/html | BUGTRAQ 20040216 EarlyImpact ProductCart shopping cart software multiple se vulnerabilities |
| EarlyImpact ProductCart Multiple Vulnerabilities | Exploit, Patch, cve.report (archive), text/html | BID 9669 |
| IBM X-Force Exchange | exchange.xforce.ibmcloud.com, text/html | XF productcart-advsearchhasp-sql-injection(15233) |
| No Description Provided | Exploit, web.archive.org, text/html, Inactive Link, Not Archived | BUGTRAQ 20040218 Re: EarlyImpact ProductCart shopping cart software multipl vulnerabilities |

| | | |
|---|---|---|
| No Description Provided | www.osvdb.org<br>Inactive Link Not Archived | OSVDB 3981 |
| dfltweb1.onamae.com – このドメインはお名前.comで取得されています。 | Exploit<br>www.s-quadra.com<br>text/plain | MISC www.s-quadra.com/advisories/Adv-20040216.txt |
| Neohapsis Archives - Full Disclosure List - #0871 - [Full-Disclosure] EarlyImpact ProductCart shopping cart software multiple security vulnerabilities | Exploit<br>web.archive.org<br>text/html<br>Inactive Link Not Archived | FULLDISC 20040216 EarlyImpact ProductCart shopping cart software multiple sec vulnerabilities |
| SecurityTracker.com Archives - ProductCart 'advSearch_h.asp' Input Validation Flaw Lets Remote Users Inject SQL to Execute Arbitrary Commands on the System | securitytracker.com<br>text/html | SECTRACK 1009085 |
| Secunia - Advisories - ProductCart SQL Injection and Cross Site Scripting Vulnerabilities | web.archive.org<br>text/html | SECUNIA 10898 |
| | www.earlyimpact.com<br>text/plain | CONFIRM www.earlyimpact.com/productcart/support/updates/ReadMe_ProductCart_Security_P |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Early Impact | Productcart | 1.5 | All | All | All |
| Application | Early Impact | Productcart | 1.5002 | All | All | All |
| Application | Early Impact | Productcart | 1.5003 | All | All | All |
| Application | Early Impact | Productcart | 1.5003r | All | All | All |
| Application | Early Impact | Productcart | 1.5004 | All | All | All |
| Application | Early Impact | Productcart | 1.6002 | All | All | All |
| Application | Early Impact | Productcart | 1.6003 | All | All | All |
| Application | Early Impact | Productcart | 1.6b | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Early Impact | Productcart | 1.6b001 | All | All | All |
| Application | Early Impact | Productcart | 1.6b002 | All | All | All |
| Application | Early Impact | Productcart | 1.6b003 | All | All | All |
| Application | Early Impact | Productcart | 1.6br | All | All | All |
| Application | Early Impact | Productcart | 1.6br001 | All | All | All |
| Application | Early Impact | Productcart | 1.6br003 | All | All | All |
| Application | Early Impact | Productcart | 2.0 | All | All | All |
| Application | Early Impact | Productcart | 2.0br000 | All | All | All |
| Application | Early Impact | Productcart | 2.5 | All | All | All |
| Application | Early Impact | Productcart | 1.5 | All | All | All |
| Application | Early Impact | Productcart | 1.5002 | All | All | All |
| Application | Early Impact | Productcart | 1.5003 | All | All | All |
| Application | Early Impact | Productcart | 1.5003r | All | All | All |
| Application | Early Impact | Productcart | 1.5004 | All | All | All |
| Application | Early Impact | Productcart | 1.6002 | All | All | All |
| Application | Early Impact | Productcart | 1.6003 | All | All | All |
| Application | Early Impact | Productcart | 1.6b | All | All | All |
| Application | Early Impact | Productcart | 1.6b001 | All | All | All |
| Application | Early Impact | Productcart | 1.6b002 | All | All | All |
| Application | Early Impact | Productcart | 1.6b003 | All | All | All |
| Application | Early Impact | Productcart | 1.6br | All | All | All |
| Application | Early Impact | Productcart | 1.6br001 | All | All | All |
| Application | Early Impact | Productcart | 1.6br003 | All | All | All |
| Application | Early Impact | Productcart | 2.0 | All | All | All |
| Application | Early Impact | Productcart | 2.0br000 | All | All | All |
| Application | Early Impact | Productcart | 2.5 | All | All | All |

cpe:2.3:a:early_impact:productcart:1.5:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.5002:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.5003:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.5003r:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.5004:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6002:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6003:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6b:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6b001:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6b002:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6b003:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6br:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6br001:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6br003:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:2.0br000:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:2.5:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.5:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.5002:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.5003:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.5003r:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.5004:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6002:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6003:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6b:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6b001:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6b002:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6b003:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6br:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6br001:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:1.6br003:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:2.0br000:*:*:*:*:*:*:*:

cpe:2.3:a:early_impact:productcart:2.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→



**CVE.report and Source URL Uptime Status status.cve.report**