



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 [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

SecurityFocus

[Exploit](#)
[www.securityfocus.com](#)
[text/html](#)

[BUGTRAQ 20040216 EarlyImpact ProductCart shopping cart software multiple security vulnerabilities](#)

EarlyImpact
ProductCart Multiple
Vulnerabilities

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

[BUG 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 multiple security vulnerabilities](#)

No Description Provided

www.osvdb.org

OSVDB 3981

Inactive Link

Not Archived

dfltwb1.onamae.com
– このドメインはお名前.comで取得されています。

Exploit

www.s-quadra.com

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

web.archive.org

text/html

Inactive Link

Not Archived

FULLDISC 20040216 EarlyImpact ProductCart shopping cart software multiple security 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

text/html

SECTrack 1009085

Secunia - Advisories - ProductCart SQL Injection and Cross Site Scripting Vulnerabilities

web.archive.org

text/html

SECUNIA 10898

www.earlyimpact.com

text/plain

CONFIRM
www.earlyimpact.com/productcart/support/updates/ReadMe_ProductCart_Security_P

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	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

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)