



CVE-2009-3112

Published on: 09/09/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:25 PM UTC

CVE-2009-3112

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

Certain versions of [Oxid Eshop](#) from [Oxidforge](#) contain the following vulnerability:

Unspecified vulnerability in OXID eShop Professional, Enterprise, and Community Edition before 4.1.0 allows remote attackers to gain administrator privileges and access the shop backend via a crafted parameter.

CVE-2009-3112 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

OXID eSales AG Security Bulletin 2009-001 - Oxidforge Wiki

[Patch](#)

[Vendor Advisory](#)

[www.oxidforge.org](#)

[text/html](#)

[CONFIRM](#)

www.oxidforge.org/wiki/Security_bulletins/2009-001

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)

Known/Annotated Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Oxidforge	Oxid Eshop	4.0.0.0_13895	All	community_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_13895	All	enterprise_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_13895	All	pro_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_13934	All	community_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_13934	All	enterprise_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_13934	All	pro_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_14260	All	community_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_14260	All	enterprise_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_14260	All	pro_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.1_14455	All	community_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.1_14455	All	enterprise_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.1_14455	All	pro_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.2_14842	All	community_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.2_14842	All	enterprise_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.2_14842	All	pro_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.2_14967	All	enterprise_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.2_14967	All	pro_edition	All
Application	Oxidforge	Oxid Eshop	4.0.1.0_15990	All	enterprise_edition	All
Application	Oxidforge	Oxid Eshop	4.0.1.0_15990	All	pro_edition	All
Application	Oxidforge	Oxid Eshop	44.0.1.0_15990	All	community_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_13895	All	community_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_13895	All	enterprise_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_13895	All	pro_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_13934	All	community_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_13934	All	enterprise_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_13934	All	pro_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_14260	All	community_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_14260	All	enterprise_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.0_14260	All	pro_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.1_14455	All	community_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.1_14455	All	enterprise_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.1_14455	All	pro_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.2_14842	All	community_edition	All
Application	Oxidforge	Oxid Eshop	4.0.0.2_14842	All	enterprise_edition	All

cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.0_13895:*:pro_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.0_13934:*:community_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.0_13934:*:enterprise_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.0_13934:*:pro_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.0_14260:*:community_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.0_14260:*:enterprise_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.0_14260:*:pro_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.1_14455:*:community_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.1_14455:*:enterprise_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.1_14455:*:pro_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.2_14842:*:community_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.2_14842:*:enterprise_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.2_14842:*:pro_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.2_14967:*:enterprise_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.2_14967:*:pro_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.1.0_15990:*:enterprise_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.1.0_15990:*:pro_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:44.0.1.0_15990:*:community_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.2_14967:*:community_edition:*:*:*:*:
cpe:2.3:a:oxidforge:oxid_eshop:4.0.0.2_14967:*:community_edition:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)