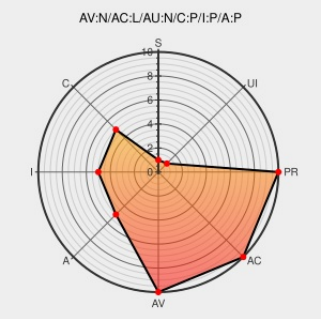
CVE-2000-1211

Published on: 12/16/2000 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:29 PM UTC

CVE-2000-1211

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



Certain versions of Zope from Zope contain the following vulnerability:

Zope 2.2.0 through 2.2.4 does not properly perform security registration for legacy names of object constructors such as DTML method objects, which could allow attackers to perform unauthorized activities.

CVE-2000-1211 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
Zope hotfix: constructor alias security	Patch, Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM www.zope.org/Products/Zope/Hotfix_2000-12-08/security_alert
MandrakeSoft Security Advisory MDKSA-2000:083 : Zope	Patch, Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	MANDRAKE MDKSA-2000:083
ISS X-Force Database: zope-legacy-names (5824): Linux zope package "legacy" names	web.archive.org, text/html, Inactive Link, Not Archived	XF zope-legacy-names(5824)
No Description Provided	www.osvdb.org	OSVDB 6282

	Inactive Link Not Archived	
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2000:125

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.

Related QID Numbers

995309 Python (Pip) Security Update for zope (GHSA-h2xh-jvpf-xq42)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zope	Zope	2.2.0	All	All	All
Application	Zope	Zope	2.2.0a1	All	All	All
Application	Zope	Zope	2.2.0b1	All	All	All
Application	Zope	Zope	2.2.0b2	All	All	All
Application	Zope	Zope	2.2.0b3	All	All	All
Application	Zope	Zope	2.2.0b4	All	All	All
Application	Zope	Zope	2.2.1	All	All	All
Application	Zope	Zope	2.2.1b1	All	All	All
Application	Zope	Zope	2.2.2	All	All	All
Application	Zope	Zope	2.2.3	All	All	All
Application	Zope	Zope	2.2.4	All	All	All
Application	Zope	Zope	2.2.0	All	All	All
Application	Zope	Zope	2.2.0a1	All	All	All
Application	Zope	Zope	2.2.0b1	All	All	All
Application	Zope	Zope	2.2.0b2	All	All	All
Application	Zope	Zope	2.2.0b3	All	All	All
Application	Zope	Zope	2.2.0b4	All	All	All
Application	Zope	Zope	2.2.1	All	All	All
Application	Zope	Zope	2.2.1b1	All	All	All
Application	Zope	Zope	2.2.2	All	All	All
Application	Zope	Zope	2.2.3	All	All	All
Application	Zope	Zope	2.2.4	All	All	All

cpe:2.3:a:zope:zope:2.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.0a1:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.0b1:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.0b2:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.0b3:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.0b4:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.1b1:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.0a1:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.0b1:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.0b2:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.0b3:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.0b4:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.1b1:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:zope:zope:2.2.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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