



CVE-2016-2242

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2016-2242
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-23 21:59:00 UTC
Updated	2018-10-09 19:59:00 UTC
Description	Exponent CMS 2.x before 2.3.7 Patch 3 allows remote attackers to execute arbitrary code via the sc parameter to install/inc

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Exponentcms	Exponent Cms	2.0.0	All	All	All
Application	Exponentcms	Exponent Cms	2.0.1	All	All	All
Application	Exponentcms	Exponent Cms	2.0.2	All	All	All
Application	Exponentcms	Exponent Cms	2.0.3	All	All	All
Application	Exponentcms	Exponent Cms	2.0.4	All	All	All
Application	Exponentcms	Exponent Cms	2.0.4	p3	All	All
Application	Exponentcms	Exponent Cms	2.0.5	All	All	All
Application	Exponentcms	Exponent Cms	2.0.5	p1	All	All
Application	Exponentcms	Exponent Cms	2.0.6	All	All	All
Application	Exponentcms	Exponent Cms	2.0.6	p2	All	All
Application	Exponentcms	Exponent Cms	2.0.7	All	All	All
Application	Exponentcms	Exponent Cms	2.0.8	All	All	All
Application	Exponentcms	Exponent Cms	2.0.8	p2	All	All
Application	Exponentcms	Exponent Cms	2.0.9	All	All	All
Application	Exponentcms	Exponent Cms	2.0.9	p5	All	All
Application	Exponentcms	Exponent Cms	2.1.0	alpha	All	All
Application	Exponentcms	Exponent Cms	2.1.1	All	All	All

Application	Exponentcms	Exponent Cms	2.1.2	All	All	All
Application	Exponentcms	Exponent Cms	2.1.3	All	All	All
Application	Exponentcms	Exponent Cms	2.1.4	All	All	All
Application	Exponentcms	Exponent Cms	2.1.4	p11	All	All
Application	Exponentcms	Exponent Cms	2.2.0	All	All	All
Application	Exponentcms	Exponent Cms	2.2.0	p5	All	All
Application	Exponentcms	Exponent Cms	2.2.1	All	All	All
Application	Exponentcms	Exponent Cms	2.2.2	All	All	All
Application	Exponentcms	Exponent Cms	2.2.2	p2	All	All
Application	Exponentcms	Exponent Cms	2.2.3	All	All	All
Application	Exponentcms	Exponent Cms	2.2.3	p14	All	All
Application	Exponentcms	Exponent Cms	2.3.0	All	All	All
Application	Exponentcms	Exponent Cms	2.3.0	p4	All	All
Application	Exponentcms	Exponent Cms	2.3.1	All	All	All
Application	Exponentcms	Exponent Cms	2.3.1	p4	All	All
Application	Exponentcms	Exponent Cms	2.3.2	All	All	All
Application	Exponentcms	Exponent Cms	2.3.2	p2	All	All
Application	Exponentcms	Exponent Cms	2.3.3	All	All	All
Application	Exponentcms	Exponent Cms	2.3.3	p1	All	All
Application	Exponentcms	Exponent Cms	2.3.4	All	All	All
Application	Exponentcms	Exponent Cms	2.3.4	p1	All	All
Application	Exponentcms	Exponent Cms	2.3.5	All	All	All
Application	Exponentcms	Exponent Cms	2.3.5	p2	All	All
Application	Exponentcms	Exponent Cms	2.3.7	All	All	All
Application	Exponentcms	Exponent Cms	2.3.8	All	All	All
Application	Exponentcms	Exponent Cms	2.0.0	All	All	All
Application	Exponentcms	Exponent Cms	2.0.1	All	All	All
Application	Exponentcms	Exponent Cms	2.0.2	All	All	All
Application	Exponentcms	Exponent Cms	2.0.3	All	All	All
Application	Exponentcms	Exponent Cms	2.0.4	All	All	All
Application	Exponentcms	Exponent Cms	2.0.4	p3	All	All
Application	Exponentcms	Exponent Cms	2.0.5	All	All	All
Application	Exponentcms	Exponent Cms	2.0.5	p1	All	All
Application	Exponentcms	Exponent Cms	2.0.6	All	All	All
Application	Exponentcms	Exponent Cms	2.0.6	p2	All	All

Application	Exponentcms	Exponent Cms	2.0.7	All	All	All
Application	Exponentcms	Exponent Cms	2.0.8	All	All	All
Application	Exponentcms	Exponent Cms	2.0.8	p2	All	All
Application	Exponentcms	Exponent Cms	2.0.9	All	All	All
Application	Exponentcms	Exponent Cms	2.0.9	p5	All	All
Application	Exponentcms	Exponent Cms	2.1.0	alpha	All	All
Application	Exponentcms	Exponent Cms	2.1.1	All	All	All
Application	Exponentcms	Exponent Cms	2.1.2	All	All	All
Application	Exponentcms	Exponent Cms	2.1.3	All	All	All
Application	Exponentcms	Exponent Cms	2.1.4	All	All	All
Application	Exponentcms	Exponent Cms	2.1.4	p11	All	All
Application	Exponentcms	Exponent Cms	2.2.0	All	All	All
Application	Exponentcms	Exponent Cms	2.2.0	p5	All	All
Application	Exponentcms	Exponent Cms	2.2.1	All	All	All
Application	Exponentcms	Exponent Cms	2.2.2	All	All	All
Application	Exponentcms	Exponent Cms	2.2.2	p2	All	All
Application	Exponentcms	Exponent Cms	2.2.3	All	All	All
Application	Exponentcms	Exponent Cms	2.2.3	p14	All	All
Application	Exponentcms	Exponent Cms	2.3.0	All	All	All
Application	Exponentcms	Exponent Cms	2.3.0	p4	All	All
Application	Exponentcms	Exponent Cms	2.3.1	All	All	All
Application	Exponentcms	Exponent Cms	2.3.1	p4	All	All
Application	Exponentcms	Exponent Cms	2.3.2	All	All	All
Application	Exponentcms	Exponent Cms	2.3.2	p2	All	All
Application	Exponentcms	Exponent Cms	2.3.3	All	All	All
Application	Exponentcms	Exponent Cms	2.3.3	p1	All	All
Application	Exponentcms	Exponent Cms	2.3.4	All	All	All
Application	Exponentcms	Exponent Cms	2.3.4	p1	All	All
Application	Exponentcms	Exponent Cms	2.3.5	All	All	All
Application	Exponentcms	Exponent Cms	2.3.5	p2	All	All
Application	Exponentcms	Exponent Cms	2.3.7	All	All	All
Application	Exponentcms	Exponent Cms	2.3.8	All	All	All

References						
Reference			Source	Link	Tags	
Patch #3 Released for V2.3.7			CONFIRM	www.exponentcms.org	Release Notes, Vendor Advisory	

SecurityFocus	BUGTRAQ	www.securityfocus.com	
File Not Found	MISC	www.htbridge.com	Exploit, Patch, Third Party Advisory
Exponent 2.3.7 PHP Code Execution ~ Packet Storm	MISC	packetstormsecurity.com	Exploit, Patch, Third Party Advisory
Security Notice: Closing an Exponent Security Vulnerability	CONFIRM	www.exponentcms.org	Exploit, Mitigation, Patch, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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