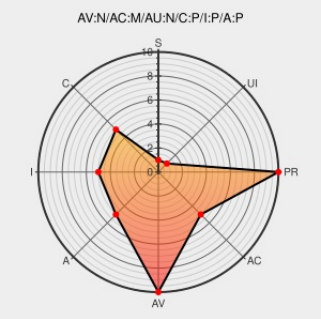
CVE-2011-4946

Published on: 08/31/2012 12:00:00 AM UTC

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

CVE-2011-4946

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



Certain versions of E107 from E107 contain the following vulnerability:

SQL injection vulnerability in e107_admin/users_extended.php in e107 before 0.7.26 allows remote attackers to execute arbitrary SQL commands via the user_field parameter.

CVE-2011-4946 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 73120
e107 SVN changelog - e107 - Free CMS | Open Source Content Management System	web.archive.org text/html Inactive Link Not Archived	CONFIRM e107.org/svn_changelog.php?version=0.7.26
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF e107-usersextended-sql-injection(68061)
File Not Found	www.htbridge.com text/html Inactive Link Not Archived	MISC www.htbridge.com/advisory/multiple_vulnerabilities_in_e107_1.html
404 Not Found	Exploit	CONFIRM

	Patch e107.svn.sourceforge.net text/html Inactive Link Not Archived	e107.svn.sourceforge.net/viewvc/e107/trunk/e107_0.7/e107_admin/users_extended.p r1=12225&r2=12306
e107 "user_field" SQL Injection Vulnerability - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 44968
oss-security - CVE-request: e107 HTB23004	www.openwall.com text/html	MLIST [oss-security] 20120328 CVE-request: e107 HTB23004
oss-security - Re: CVE-request: e107 HTB23004	www.openwall.com text/html	MLIST [oss-security] 20120328 Re: CVE-request: e107 HTB23004

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	E107	E107	0.7.0	All	All	All
Application	E107	E107	0.7.1	All	All	All
Application	E107	E107	0.7.10	All	All	All
Application	E107	E107	0.7.11	All	All	All
Application	E107	E107	0.7.12	All	All	All
Application	E107	E107	0.7.13	All	All	All
Application	E107	E107	0.7.14	All	All	All
Application	E107	E107	0.7.15	All	All	All
Application	E107	E107	0.7.16	All	All	All
Application	E107	E107	0.7.17	All	All	All
Application	E107	E107	0.7.18	All	All	All
Application	E107	E107	0.7.19	All	All	All
Application	E107	E107	0.7.2	All	All	All
Application	E107	E107	0.7.20	All	All	All
Application	E107	E107	0.7.21	All	All	All
Application	E107	E107	0.7.22	All	All	All
Application	E107	E107	0.7.3	All	All	All
Application	E107	E107	0.7.4	All	All	All

Application	E107	E107	0.7.5	All	All	All
Application	E107	E107	0.7.6	All	All	All
Application	E107	E107	0.7.7	All	All	All
Application	E107	E107	0.7.8	All	All	All
Application	E107	E107	0.7.9	All	All	All
Application	E107	E107	All	All	All	All
Application	E107	E107	0.7.0	All	All	All
Application	E107	E107	0.7.1	All	All	All
Application	E107	E107	0.7.10	All	All	All
Application	E107	E107	0.7.11	All	All	All
Application	E107	E107	0.7.12	All	All	All
Application	E107	E107	0.7.13	All	All	All
Application	E107	E107	0.7.14	All	All	All
Application	E107	E107	0.7.15	All	All	All
Application	E107	E107	0.7.16	All	All	All
Application	E107	E107	0.7.17	All	All	All
Application	E107	E107	0.7.18	All	All	All
Application	E107	E107	0.7.19	All	All	All
Application	E107	E107	0.7.2	All	All	All
Application	E107	E107	0.7.20	All	All	All
Application	E107	E107	0.7.21	All	All	All
Application	E107	E107	0.7.22	All	All	All
Application	E107	E107	0.7.3	All	All	All
Application	E107	E107	0.7.4	All	All	All
Application	E107	E107	0.7.5	All	All	All
Application	E107	E107	0.7.6	All	All	All
Application	E107	E107	0.7.7	All	All	All
Application	E107	E107	0.7.8	All	All	All
Application	E107	E107	0.7.9	All	All	All

cpe:2.3:a:e107:e107:0.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.10:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.11:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.12:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.13:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.14:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.15:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.16:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.17:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.18:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.19:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.2:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.20:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.21:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.22:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.3:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.4:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.5:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.6:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.7:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.8:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.9:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:*:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.10:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.11:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.12:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.13:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.14:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.15:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.16:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.17:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.18:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.19:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.2:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.20:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.21:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.22:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.3:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.4:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.5:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.6:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.7:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.8:*:*:*:*:*:*:*:

cpe:2.3:a:e107:e107:0.7.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→