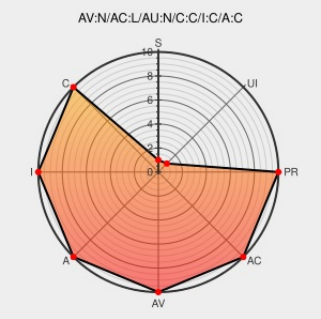
CVE-2011-2148

Published on: 05/20/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:22 PM UTC

CVE-2011-2148

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



Certain versions of Smarterstats from Smartertools contain the following vulnerability:

Admin/frmSite.aspx in the SmarterTools SmarterStats 6.0 web server allows remote attackers to execute arbitrary commands via vectors involving a leading and trailing & (ampersand) character, and (1) an STTTState cookie, (2) the ctl00%24MPH%24txtAdminNewPassword_SettingText parameter, (3) the ctl00%24MPH%24txtSmarterLogDirectory parameter, (4) the ctl00%24MPH%24ucSiteSeoSearchEngineSettings%24chklistEngines_SettingCheckBox%241 parameter, (5) the ctl00%24MPH%24ucSiteSeoSettings%24txtSeoMaxKeywords_SettingText parameter, or (6) the ctl00_MPH_grdLogLocations_HiddenLSR parameter, related to an "OS command injection" issue.

CVE-2011-2148 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF smarterstats-frmsite-command-exec(67834)
SQL Injection, XML Injection, OS Command Injection, SmarterStats 6.0	xss.cx text/html	MISC xss.cx/examples/smarterstats-60-oscommandinjection-directorytraversal-xml-sqlinjection.html.html

US-CERT Vulnerability Note VU#240150 - SmarterTools default basic web server vulnerabilities	US Government Resource www.kb.cert.org text/html	CERT-VN VU#240150
SmarterTools Inc. Information for VU#240150	US Government Resource www.kb.cert.org text/html	MISC www.kb.cert.org/vuls/id/MORO-8GYQR4

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Smartertools	Smarterstats	6.0	All	All	All
Application	Smartertools	Smarterstats	6.0	All	All	All

cpe:2.3:a:smartertools:smarterstats:6.0:*:*:*:*:*:*:*

cpe:2.3:a:smartertools:smarterstats:6.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→