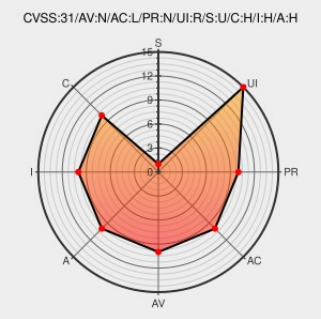
CVE-2012-2629

Published on: 02/19/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:27 PM UTC

CVE-2012-2629

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



Certain versions of Axous from Axous contain the following vulnerability:

Multiple cross-site request forgery (CSRF) and cross-site scripting (XSS) vulnerabilities in Axous 1.1.1 and earlier allow remote attackers to hijack the authentication of administrators for requests that (1) add an administrator account via an addnew action to admin/administrators_add.php; or (2) conduct cross-site scripting (XSS) attacks via the page_title parameter to admin/content_pages_edit.php; the (3) category_name[] parameter to admin/products_category.php; the (4) site_name, (5) seo_title, or (6) meta_keywords parameter to admin/settings_siteinfo.php; the (7) company_name, (8) address1, (9) address2, (10) city, (11) state, (12) country, (13) author_first_name, (14) author_last_name, (15) author_email, (16) contact_first_name, (17) contact_last_name, (18) contact_email, (19) general_email, (20) general_phone, (21) general_fax, (22) sales_email, (23) sales_phone, (24) support_email, or (25) support_phone parameter to admin/settings_company.php; or the (26) system_email, (27) sender_name, (28) smtp_server, (29) smtp_username, (30) smtp_password, or (31) order_notice_email parameter to admin/settings_email.php.

CVE-2012-2629 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

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
Axous 1.1.1 Multiple Vulnerabilities (CSRF - Persistent XSS)	Exploit, Third Party Advisory, VDB Entry, www.exploit-db.com, Proof of Concept, text/html	MISC www.exploit-db.com/exploits/18886
Axous 1.1.1 Cross Site Request Forgery / Cross Site Scripting ≈ Packet Storm	Exploit, Third Party Advisory, VDB Entry, packetstormsecurity.com, text/html	MISC packetstormsecurity.com/files/112748/Axous-1.1.1-Cross-Site-Request-Forgery-Cross-Site-Scripting.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Axous	Axous	All	All	All	All

cpe:2.3:a:axous:axous:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→