



CVE-2018-1000629

Published on: 12/28/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:30 PM UTC

CVE-2018-1000629

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [V2i Hub](#) from [Battelle](#) contain the following vulnerability:

Battelle V2I Hub 2.5.1 is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by `api/SystemConfigActions.php?action=add` and the `index.php` script. A remote attacker could exploit this vulnerability using the `parameterName` or `_login_username` parameter in a specially-crafted

URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

CVE-2018-1000629 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

