National Critical Information Infrastructure Protection Centre
CVE Report
CV Scoring Scale : 3-10   **01 Nov –30 Nov 2018**   **Vol. 05 No.22**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Application					
Centos-webpanel					
Centos Web Panel					
CSRF	20-11-2018	6.8	CentOS-WebPanel.com (aka CWP) CentOS Web Panel through 0.9.8.740 allows CSRF via admin/index.php?module=rootpwd, as demonstrated by changing the root password. **CVE-ID:CVE-2018-18773**	https://www.exploit-db.com/exploits/45822/	A-Cen-Cento/03-12-18/1
CSRF	20-11-2018	6.8	CentOS-WebPanel.com (aka CWP) CentOS Web Panel through 0.9.8.740 allows CSRF via admin/index.php?module=send_ssh, as demonstrated by executing an arbitrary OS command. **CVE-ID:CVE-2018-18772**	https://www.exploit-db.com/exploits/45822/	A-Cen-Cento/03-12-18/2
XSS	20-11-2018	4.3	CentOS-WebPanel.com (aka CWP) CentOS Web Panel through 0.9.8.740 allows XSS via the admin/index.php module parameter. **CVE-ID:CVE-2018-18774**	https://www.exploit-db.com/exploits/45822/	A-Cen-Cento/03-12-18/3
Cisco					
Prime Service Catalog					
Execute Code XSS	08-11-2018	3.5	A vulnerability in the web-based management interface of Cisco Prime Service Catalog could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181107-psc-xss	A-Cis-Prime/03-12-18/4

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			interface. The vulnerability is due to insufficient validation of user-supplied input that is processed by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive browser-based information. **CVE-ID:CVE-2018-15451**		
IBM					
Maximo Asset Management					
XSS	09-11-2018	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 151330. **CVE-ID:CVE-2018-1872**	https://www.ibm.com/support/docview.wss?uid=ibm10737461,https://exchange.xforce.ibmcloud.com/vulnerabilities/151330	A-IBM-Maxim/03-12-18/5
Rational Quality Manager					
XSS	02-11-2018	3.5	IBM Quality Manager (RQM) 5.0 through 5.0.2 and 6.0 through 6.0.6 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	https://exchange.xforce.ibmcloud.com/vulnerabilities/132929	A-IBM-Ratio/03-12-18/6

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 132929. **CVE-ID:CVE-2017-1609**		
Websphere Application Server					
XSS	12-11-2018	4.3	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 149428. **CVE-ID:CVE-2018-1798**	https://exchange.xforce.ibmcloud.com/vulnerabilities/149428	A-IBM-Websp/03-12-18/7
XSS	15-11-2018	4.3	The Installation Verification Tool of IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 144588 **CVE-ID:CVE-2018-1643**	https://exchange.xforce.ibmcloud.com/vulnerabilities/144588,https://www.ibm.com/support/docview.wss?uid=ibm10716857	A-IBM-Websp/03-12-18/8
SAP					
Businessobjects Bi Platform					
XSS	13-11-2018	4.3	SAP BusinessObjects Business Intelligence Platform (BIWorkspace), versions 4.1	https://wiki.scn.sap.com/wiki/pages/viewpage.actio	A-SAP-Busin/03-12-18/9

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			and 4.2, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. **CVE-ID:CVE-2018-2479**	n?pageId=503809 832,https://launc hpad.support.sap. com/#/notes/26 76094	
Wuzhicms					
Wuzhi Cms					
XSS	05-11-2018	3.5	An issue was discovered in WUZHI CMS 4.1.0. There is stored XSS in index.php?m=core&f=index via an ontoggle attribute to details/open/ within a second input field. **CVE-ID:CVE-2018-18938**	https://github.co m/wuzhicms/wu zhicms/issues/15 8	A-Wuz-Wuzhi/03-12-18/11
Wuzhi Cms Project					
Wuzhi Cms					
XSS	05-11-2018	3.5	An issue was discovered in WUZHI CMS 4.1.0. There is stored XSS in index.php?m=core&f=index via a seventh input field. **CVE-ID:CVE-2018-18939**	https://github.co m/wuzhicms/wu zhicms/issues/15 9	A-Wuz-Wuzhi/03-12-18/10

CV Scoring Scale (CVSS)		3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;