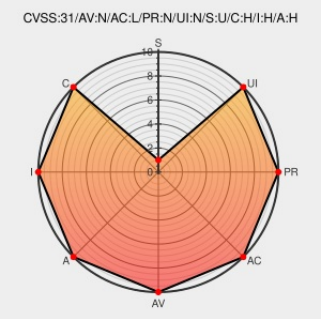
CVE-2019-3396

Published on: 03/25/2019 12:00:00 AM UTC

Last Modified on: 12/13/2021 04:05:00 PM UTC

CVE-2019-3396

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



Certain versions of Confluence from Atlassian contain the following vulnerability:

The Widget Connector macro in Atlassian Confluence Server before version 6.6.12 (the fixed version for 6.6.x), from version 6.7.0 before 6.12.3 (the fixed version for 6.12.x), from version 6.13.0 before 6.13.3 (the fixed version for 6.13.x), and from version 6.14.0 before 6.14.2 (the fixed version for 6.14.x), allows remote attackers to achieve path traversal and remote code execution on a Confluence Server or Data Center instance via server-side template injection.

CVE-2019-3396 has been assigned by security@atlassian.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

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
Atlassian Confluence Widget	Exploit	EXPLOIT-DB-46731

Atlassian Confluence Widget Connector Macro - Velocity Template Injection (Metasploit) - Multiple remote Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 46731
Atlassian Confluence Widget Connector Macro Velocity Template Injection	Exploit Third Party Advisory VDB Entry www.rapid7.com text/html	MISC www.rapid7.com/db/modules/exploit/multi/http/confluence_widget_connector
[CONFSERVER-57974] Remote code execution via Widget Connector macro - CVE-2019-3396 - Create and track feature requests for Atlassian products.	Issue Tracking Patch Vendor Advisory jira.atlassian.com text/html	MISC jira.atlassian.com/browse/CONFSERVER-57974
Atlassian Confluence Widget Connector Macro Velocity Template Injection ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/152568/Atlassian-Confluence-Widget-Connector-Macro-Velocity-Template-Injection.html
Atlassian Confluence 6.12.1 Template Injection ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/161065/Atlassian-Confluence-6.12.1-Template-Injection.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Confluence	All	All	All	All
Application	Atlassian	Confluence	All	All	All	All
Application	Atlassian	Confluence Server	All	All	All	All

cpe:2.3:a:atlassian:confluence:*:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:confluence:*:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

@pwnwikiorg	CVE-2019-3396 Atlassian Confluence 路徑穿越&命令執行漏洞 pwnwiki.org/index.php?titl…	2021-05-05 06:56:51
@simonryoung1	Cybercriminals have found a new method for abusing CVE-2019-3396: exploiting it to deliver a cryptocurrency-mining… twitter.com/i/web/status/1…	2021-07-31 12:05:07
@bad_packets	@campuscodi C2 active since 2021-03-19T04:19:47Z Also targeting: – CVE-2019-3396 (Confluence RCE) – CVE-2019-10758… twitter.com/i/web/status/1…	2021-08-12 18:16:45
@polo_nmh	Cybercriminals have found a new method for abusing CVE-2019-3396: exploiting it to deliver a cryptocurrency-mining… twitter.com/i/web/status/1…	2021-08-18 12:57:58
@ldap389	@uuallan ?CVE-2010-0738: varonis.com/blog/new-samsa… ?CVE-2019-3396: alertlogic.com/blog/active-ex…	2021-09-12 18:54:14
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #trojan #0day #malware	2021-09-15 15:26:57
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #leak #cyberintelligence #hacker	2021-09-15 15:27:56
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #http[:] #cyberattack #[.]onion	2021-09-15 15:28:40
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #http[:] #botnet #ransomware	2021-09-15 15:29:35
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #malware #hacker #infosec	2021-09-15 15:30:26
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #hacking #http[:] #cybersecurity	2021-09-15 15:31:10
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #cyberattack #hacking #malware	2021-09-15 15:31:34
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #[.]onion #CVE #databreach	2021-09-15 15:31:54
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #ransomware #http[:] #ransomware	2021-09-15 15:32:14
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #cyberintelligence #hacker #cybersecurity	2021-09-15 15:32:31
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #0day #malware #[.]onion	2021-09-15 15:32:47
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #cyberthreat #leak #cyberattack	2021-09-15 15:32:56
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #trojan #cyberthreat #databreach	2021-09-15 15:33:07
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #[.]onion #Belgium #[.]onion	2021-09-15 15:33:16
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #[.]onion #cyberattack #ransomware	2021-09-15 15:33:27
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #http[:] #Belgium #0day	2021-09-15 15:33:35
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #backdoor #cyberintelligence #cybersecurity	2021-09-15 15:33:42
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #trojan #databreach #botnet	2021-09-15 15:33:48

@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #http[:] #rootkit #hxxp	2021-09-15 15:33:57
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #leak #hacker #malware	2021-09-15 15:34:02
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #malware #phishing #[.]onion	2021-09-15 15:34:13
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #backdoor #hacker #backdoor	2021-09-15 15:34:50
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #malware #databreach #hxxp	2021-09-15 15:34:58
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #malware #botnet #CVE	2021-09-15 15:35:03
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #http[:] #infosec #botnet	2021-09-15 15:35:08
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #infosec #backdoor #hacking	2021-09-15 15:35:14
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #0day #trojan #hacker	2021-09-15 15:35:20
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #ransomware #hacker #leak	2021-09-15 15:35:25
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #Belgium #http[:] #Belgium	2021-09-15 15:35:35
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #trojan #0day #[.]onion	2021-09-15 15:36:00
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #backdoor #cyberthreat #leak	2021-09-15 15:36:05
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #phishing #phishing #malware	2021-09-15 15:36:14
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #hacker #cybersecurity #hxxp	2021-09-15 15:36:26
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #0day #rootkit #0day	2021-09-15 15:36:35
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #cyberintelligence… twitter.com/i/web/status/1…	2021-09-15 15:36:45
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #backdoor #cyberattack #cybersecurity	2021-09-15 15:36:50
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #botnet #Belgium #hacker	2021-09-15 15:36:57
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #Belgium #botnet #databreach	2021-09-15 15:37:13
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #hxxp #malware #cyberthreat	2021-09-15 15:37:20
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ # [.]onion #http[:] #Belgium	2021-09-15 15:37:32
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #cyberthreat #malware #Belgium	2021-09-15 15:37:44

@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #malware #backdoor #cyberattack	2021-09-15 15:37:56
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #cyberthreat #leak #hxxp	2021-09-15 15:38:03
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #leak #infosec #databreach	2021-09-15 15:38:08
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #CVE #Belgium #cybersecurity	2021-09-15 15:38:14
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #ransomware #databreach #infosec	2021-09-15 15:38:20
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #cyberthreat #botnet #trojan	2021-09-15 15:38:24
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #hxxp #hacker #infosec	2021-09-15 15:38:31
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #cyberintelligence #cyberintelligence #0day	2021-09-15 15:38:35
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #cybersecurity #hxxp #CVE	2021-09-15 15:38:40
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #backdoor #botnet #[.]onion	2021-09-15 15:38:44
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #http[:] #cybersecurity #http[:]	2021-09-15 15:38:50
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #botnet #backdoor #[.]onion	2021-09-15 15:38:58
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #infosec #cybersecurity #ransomware	2021-09-15 15:39:04
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #http[:] #ransomware #backdoor	2021-09-15 15:39:08
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #phishing #trojan #rootkit	2021-09-15 15:39:17
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #leak #databreach #hxxp	2021-09-15 15:39:24
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #databreach #backdoor #hacker	2021-09-15 15:39:31
@01_security_01	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396) Analysis - paper.seebug.org/886/ #leak #backdoor #cyberintelligence	2021-09-15 15:40:11
@aacevesj	Cybercriminals have found a new method for abusing CVE-2019-3396: exploiting it to deliver a cryptocurrency-mining… twitter.com/i/web/status/1…	2021-10-04 03:58:06
@tuhin1729_	(5/n) 8. CVE-2019-3396(Path Traversal & RCE): POST /rest/tinymce/1/macro/preview HTTP/1.1 Host: JIRA ... {"conten… twitter.com/i/web/status/1…	2021-10-05 06:55:11
@OPOSEC	SSTI and RCE in Confluence Server via Widget Connector (CVE-2019-3396). bit.ly/2X5eTCX (+) More:… twitter.com/i/web/status/1…	2021-11-17 08:00:01
@buaqbot	Confluence CVE-2019-3396 & CVE-2021-26084漏洞分析 ift.tt/3G1LpNq ift.tt/3FTwncl	2022-01-06 07:32:55
@Recon_InfoSec	For teams dealing with CVE-2022-26134, see this blog post which analyzes a previous Confluence RCE (CVE-2019-3396).… twitter.com/i/web/status/1…	2022-06-03 00:54:09

/r/sysadmin	25 vulnerabilities exploited by Chinese state-sponsored hackers	2020-10-21 11:41:34
/r/cybersecurity	25 vulnerabilities exploited by Chinese state-sponsored hackers	2020-10-21 11:37:21

← Previous ID

Next ID→