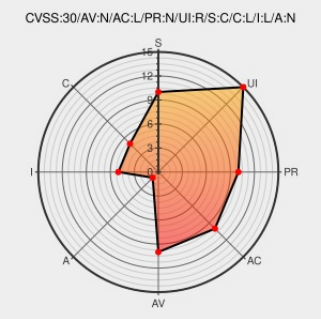
CVE-2017-9506

Published on: 08/23/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:56 PM UTC

CVE-2017-9506

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



Certain versions of Oauth from Atlassian contain the following vulnerability:

The IconUriServlet of the Atlassian OAuth Plugin from version 1.3.0 before version 1.9.12 and from version 2.0.0 before version 2.0.4 allows remote attackers to access the content of internal network resources and/or perform an XSS attack via Server Side Request Forgery (SSRF).

CVE-2017-9506 has been assigned by security@atlassian.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Atlassian** - **Atlassian OAuth Plugin** version **From version 1.3.0 before version 1.9.12 and from version 2.0.0 before version 2.0.4.**

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

Piercing the Veil: Server Side Request Forgery to NIPRNet access	Broken Link Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC medium.com/bugbountywriteup/piercing-the-veil-server-side-request-forgery-to-niprnet-access-171018bca2c3
Don't Panic: There is a proxy in your Atlassian Product! (CVE-2017-9506)	Exploit Third Party Advisory dontpanic.42.nl text/html	MISC dontpanic.42.nl/2017/12/there-is-proxy-in-your-atlassian.html
ZeroSecurity na Twitterze: "Abusing CVE-2017-9506 to access internal services and #hacking the Department of the Defense in the process #DOD #Exploit #InfoSec https://t.co/WjMlHGYqt8"	Exploit Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/Zer0Security/status/983529439433777152
[OAUTH-344] The icon-uri servlet allows arbitrary HTTP requests to be proxied - CVE-2017-9506 - Ecosystem Jira	Issue Tracking Vendor Advisory ecosystem.atlassian.net text/html	MISC ecosystem.atlassian.net/browse/OAUTH-344
Ankit Anubhav on Twitter: "#JIRA users, attention. Attackers are using JIRA exploit CVE-2017-9506 to get inside your network for data theft. Its sort of an open redirect vuln, but in some cases it can even redirect to internal link-local address , using which they are trying to access AWS creds. (1/n)… https://t.co/NaZxNyXZaL"	Exploit Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/ankit_anubhav/status/973566620676382721

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2017-9506

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Oauth	1.3.0	All	All	All
Application	Atlassian	Oauth	1.3.1	All	All	All
Application	Atlassian	Oauth	1.3.10	All	All	All
Application	Atlassian	Oauth	1.3.2	All	All	All
Application	Atlassian	Oauth	1.3.3	All	All	All
Application	Atlassian	Oauth	1.3.4	All	All	All
Application	Atlassian	Oauth	1.3.5	All	All	All
Application	Atlassian	Oauth	1.3.6	All	All	All
Application	Atlassian	Oauth	1.3.7	All	All	All

Application	Atlassian	Oauth	1.3.8	All	All	All
Application	Atlassian	Oauth	1.3.9	All	All	All
Application	Atlassian	Oauth	1.4.0	All	All	All
Application	Atlassian	Oauth	1.4.0	m1	All	All
Application	Atlassian	Oauth	1.4.0	m2	All	All
Application	Atlassian	Oauth	1.4.1	All	All	All
Application	Atlassian	Oauth	1.5.0	All	All	All
Application	Atlassian	Oauth	1.5.0	m1	All	All
Application	Atlassian	Oauth	1.5.0	m3	All	All
Application	Atlassian	Oauth	1.6.0	All	All	All
Application	Atlassian	Oauth	1.6.0	m1	All	All
Application	Atlassian	Oauth	1.6.0	m4	All	All
Application	Atlassian	Oauth	1.6.1	All	All	All
Application	Atlassian	Oauth	1.7.0	All	All	All
Application	Atlassian	Oauth	1.8.0	All	All	All
Application	Atlassian	Oauth	1.8.0	m1	All	All
Application	Atlassian	Oauth	1.8.1	All	All	All
Application	Atlassian	Oauth	1.8.2	All	All	All
Application	Atlassian	Oauth	1.8.3	All	All	All
Application	Atlassian	Oauth	1.8.4	All	All	All
Application	Atlassian	Oauth	1.8.5	All	All	All
Application	Atlassian	Oauth	1.9.0	All	All	All
Application	Atlassian	Oauth	1.9.0	m1	All	All
Application	Atlassian	Oauth	1.9.0	m2	All	All
Application	Atlassian	Oauth	1.9.1	All	All	All
Application	Atlassian	Oauth	1.9.10	All	All	All
Application	Atlassian	Oauth	1.9.11	All	All	All
Application	Atlassian	Oauth	1.9.2	All	All	All
Application	Atlassian	Oauth	1.9.3	All	All	All
Application	Atlassian	Oauth	1.9.4	All	All	All
Application	Atlassian	Oauth	1.9.5	All	All	All
Application	Atlassian	Oauth	1.9.6	All	All	All
Application	Atlassian	Oauth	1.9.7	All	All	All
Application	Atlassian	Oauth	1.9.8	All	All	All
Application	Atlassian	Oauth	1.9.9	All	All	All
Application	Atlassian	Oauth	2.0.0	All	All	All

Application	Atlassian	Oauth	2.0.1	All	All	All
Application	Atlassian	Oauth	2.0.2	All	All	All
Application	Atlassian	Oauth	2.0.3	All	All	All
Application	Atlassian	Oauth	1.3.0	All	All	All
Application	Atlassian	Oauth	1.3.1	All	All	All
Application	Atlassian	Oauth	1.3.10	All	All	All
Application	Atlassian	Oauth	1.3.2	All	All	All
Application	Atlassian	Oauth	1.3.3	All	All	All
Application	Atlassian	Oauth	1.3.4	All	All	All
Application	Atlassian	Oauth	1.3.5	All	All	All
Application	Atlassian	Oauth	1.3.6	All	All	All
Application	Atlassian	Oauth	1.3.7	All	All	All
Application	Atlassian	Oauth	1.3.8	All	All	All
Application	Atlassian	Oauth	1.3.9	All	All	All
Application	Atlassian	Oauth	1.4.0	All	All	All
Application	Atlassian	Oauth	1.4.0	m1	All	All
Application	Atlassian	Oauth	1.4.0	m2	All	All
Application	Atlassian	Oauth	1.4.1	All	All	All
Application	Atlassian	Oauth	1.5.0	All	All	All
Application	Atlassian	Oauth	1.5.0	m1	All	All
Application	Atlassian	Oauth	1.5.0	m3	All	All
Application	Atlassian	Oauth	1.6.0	All	All	All
Application	Atlassian	Oauth	1.6.0	m1	All	All
Application	Atlassian	Oauth	1.6.0	m4	All	All
Application	Atlassian	Oauth	1.6.1	All	All	All
Application	Atlassian	Oauth	1.7.0	All	All	All
Application	Atlassian	Oauth	1.8.0	All	All	All
Application	Atlassian	Oauth	1.8.0	m1	All	All
Application	Atlassian	Oauth	1.8.1	All	All	All
Application	Atlassian	Oauth	1.8.2	All	All	All
Application	Atlassian	Oauth	1.8.3	All	All	All
Application	Atlassian	Oauth	1.8.4	All	All	All
Application	Atlassian	Oauth	1.8.5	All	All	All
Application	Atlassian	Oauth	1.9.0	All	All	All
Application	Atlassian	Oauth	1.9.0	m1	All	All

Application	Atlassian	Oauth	1.9.0	m2	All	All
Application	Atlassian	Oauth	1.9.1	All	All	All
Application	Atlassian	Oauth	1.9.10	All	All	All
Application	Atlassian	Oauth	1.9.11	All	All	All
Application	Atlassian	Oauth	1.9.2	All	All	All
Application	Atlassian	Oauth	1.9.3	All	All	All
Application	Atlassian	Oauth	1.9.4	All	All	All
Application	Atlassian	Oauth	1.9.5	All	All	All
Application	Atlassian	Oauth	1.9.6	All	All	All
Application	Atlassian	Oauth	1.9.7	All	All	All
Application	Atlassian	Oauth	1.9.8	All	All	All
Application	Atlassian	Oauth	1.9.9	All	All	All
Application	Atlassian	Oauth	2.0.0	All	All	All
Application	Atlassian	Oauth	2.0.1	All	All	All
Application	Atlassian	Oauth	2.0.2	All	All	All
Application	Atlassian	Oauth	2.0.3	All	All	All

cpe:2.3:a:atlassian:oauth:1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.4.0:m1:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.4.0:m2:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.5.0:m1:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.5.0:m3:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.6.0:m1:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.6.0:m4:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.8.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.8.0:m1:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.8.1:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.8.2:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.8.3:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.8.4:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.0:m1:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.0:m2:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.1:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.10:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.11:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.3:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.4:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.5:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.6:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.7:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.8:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.9.9:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:2.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:2.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.4.0:m1:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.4.0:m2:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.5.0:m1:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.5.0:m3:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.6.0:m1:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.6.0:m4:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.8.0:*:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.8.0:m1:*:*:*:*:*:*:

cpe:2.3:a:atlassian:oauth:1.8.0:m1:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.8.1:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.8.2:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.8.3:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.8.4:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.8.5:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.0:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.0:m1:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.0:m2:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.1:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.10:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.11:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.2:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.3:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.4:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.5:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.6:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.7:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.8:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:1.9.9:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:2.0.0:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:2.0.1:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:2.0.2:*:*:*:*:*:*:*

cpe:2.3:a:atlassian:oauth:2.0.3:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report