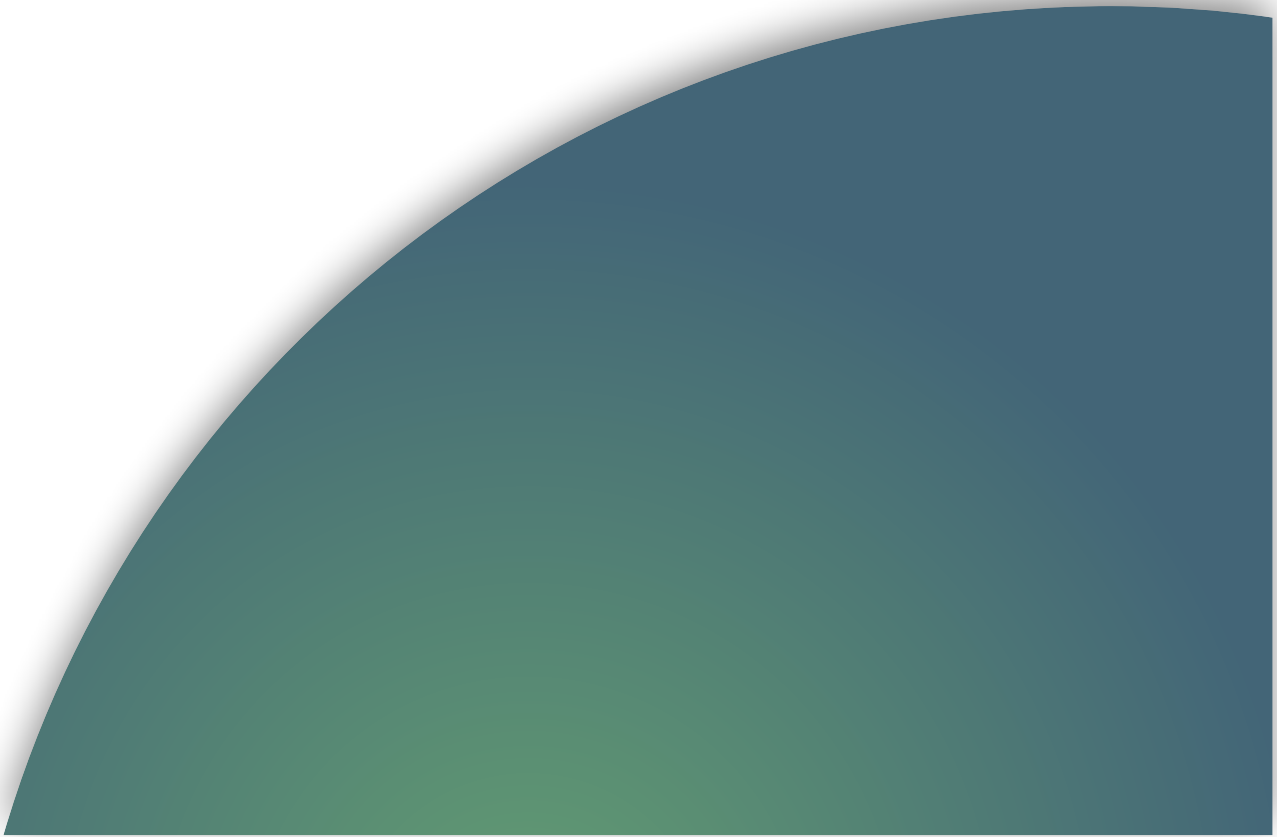


Do you use the API?

Do you control the CI/CD network access?

TestLink Plugin stores credentials in plain text

SECURITY-1428 / CVE-2019-10378

TestLink Plugin stores credentials unencrypted in its global configuration file `hudson.plugins.testlink.TestLinkBuilder.xml` on the Jenkins master. These credentials can be viewed by users with access to the master file system.

As of publication of this advisory, there is no fix.

Mask Passwords Plugin shows plain text passwords in global configuration form fields

SECURITY-157 / CVE-2019-10370
Mask Passwords Plugin allows specifying passwords to be provided to builds in the global Jenkins configuration.

While the passwords are stored encrypted on disk, they are transmitted in plain text as part of the configuration form. This can result in exposure of the password through browser extensions, cross-site scripting vulnerabilities, and similar situations.

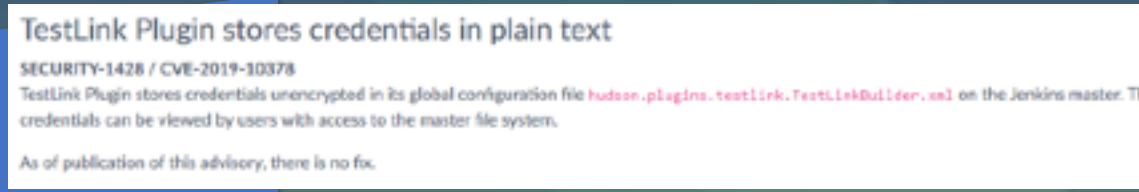
As of publication of this advisory, there is no fix.

Disable access from unnecessary places with a firewall. Do not install vulnerable Plugins.

Keep API Safe!

Keep API Safe!

- Do you use the API?
- Do you control the CI/CD network access?



TestLink Plugin stores credentials in plain text

SECURITY-1428 / CVE-2019-10378

TestLink Plugin stores credentials unencrypted in its global configuration file `hudson.plugins.testlink.TestLinkBuilder.xml` on the Jenkins master. T
credentials can be viewed by users with access to the master file system.

As of publication of this advisory, there is no fix.

Mask Passwords Plugin shows plain text passwords in global configuration form fields

SECURITY-157 / CVE-2019-10370

Mask Passwords Plugin allows specifying passwords to be provided to builds in the global Jenkins configuration.

While the passwords are stored encrypted on disk, they are transmitted in plain text as part of the configuration form. This can result in exposure of the password through browser extensions, cross-site scripting vulnerabilities, and similar situations.

As of publication of this advisory, there is no fix.

Disable access from unnecessary places with a firewall. Do not install vulnerable Plugins.

The SOURCE CODE ransomware!

- Do you keep your source code repository safe?
- Do you keep your developers machines safe?
- Do you backup your code?