



## Pluralsight customer statement on log4j

---

Tags: [Skills](#) [ACG](#) [Flow](#) [Flow on-prem](#)

In this article

[Skills statement](#)

[Flow Cloud statement](#)

[Flow Enterprise Server statement](#)

[A Cloud Guru statement](#)

---

### Skills statement

The Pluralsight Skills team has remediated all known instances of log4j as prescribed by the [NCSC guidelines \(external site, opens in new tab\)](#). In addition, we have investigated our third-party commercial dependencies, each of which has been remediated or we've deemed to have no impact to Skills or Skills customers. We are also following NCSC guidelines for compromise detection and mitigation, and have identified zero successful exploits. We are continuing to follow the NCSC guidelines which includes updating to the latest version and as their guidance is updated, we are taking immediate action to remediate.

Additionally, we know many of you and your teams are investigating and remediating the effects of log4j. If you'd like to learn more about what it is, how to identify if you've been affected, and how to remediate please check out this free video course: [Log4j Vulnerability: What You Should Know \(opens in new tab\)](#).

[back to top](#)

---

### Flow Cloud statement

The Pluralsight Flow team has remediated all known instances of log4j as prescribed by the [NCSC guidelines \(external site, opens in new tab\)](#). In addition, we have investigated our third-party commercial dependencies, each of which has been remediated or we've deemed to have no impact to Flow or Flow customers. We are also following NCSC guidelines for compromise detection and mitigation, and have identified zero successful exploits. We are continuing to follow the NCSC guidelines which includes updating to the latest version and as their guidance is updated, we are taking immediate action to remediate.

[back to top](#)

---

### Flow Enterprise Server statement

The Pluralsight Flow teams have identified instances of log4j and are actively remediating all risks as prescribed

by the [NCSC guidelines \(external site, opens in new tab\)](#) . For the Pluralsight Flow Enterprise Server product, customers can remediate their running system through JVM configurations available on the management console. See [instructions for JVM configurations](#).

Additionally, we have released an upgrade that will mitigate all known product risks, including start-up modules. We recommend that all customers perform an upgrade at their earliest, reasonable convenience.

Once customers are on [2021.3.1-2](#) or higher, the JVM remediation is no longer required. We will continue to address new vulnerabilities with new releases as necessary.

[back to top](#)

---

## A Cloud Guru statement

The A Cloud Guru team has remediated all known instances of log4j as prescribed by the [NCSC guidelines \(external site, opens in new tab\)](#). In addition, we have investigated our third-party commercial dependencies, each of which has been remediated or we've deemed to have no impact to A Cloud Guru or A Cloud Guru customers. We are also following NCSC guidelines for compromise detection and mitigation, and have identified zero successful exploits. We are continuing to follow the NCSC guidelines which includes updating to the latest version and as their guidance is updated, we are taking immediate action to remediate.

---

If you need help, please email [support@pluralsight.com](mailto:support@pluralsight.com) for 24/7 assistance.