UPDATE - Actian Security Alert

Communication Content

December 15, 2021

Information security is of the utmost importance to Actian. A new vulnerability dated December 10, 2021, Oracle Corporation Oracle Security Alert Advisory - CVE-2021-44228 identifies a vulnerability in Apache Log4j. It is remotely exploitable without authentication, i.e., may be exploited over a network without the need for a username and password. The exploitable versions of Apache Log4j are versions 2.0 - 2.14.1

Please be advised that Actian is doing an extensive internal review of our software products to understand how the vulnerability impacts each product, and we will provide updates as more information becomes available. At the time of writing, Actian has given this vulnerability a security threat level of "low" given its level of impact.

Actian Products that have been identified as impacted by this vulnerability and use Apache Log4j v2.0 or greater.

- Actian DataConnect Version 12 (only)
  - The core Actian DataConnect V12 functionality does not use Log4j. Data Profiler is an application within Actian DataConnect V12 and uses affected version Apache Log4j, v2.14.1.
  - Recommended Actions: Actian DataConnect V12 was removed from our download site on December 13, 2021 and will be replaced by a remediated version which we expect to make available in the coming days. We recommend discontinuing your use of DataConnect V12 Data Profiler until the update is released to our download site.
- Actian X 11.2; Ingres 11.2 and Vector 6.2 (only)
  - The core Ingres and Vector engines do not use Log4j, however Actian Director, a GUI management tool included with these products, uses affected version 2.14.1
  - Recommended Actions: Please discontinue the use of Actian Director immediately until an updated version is released via our download site.

Actian Products that use Log4j but not the affected versions.

- Actian DataCloud (Integration Manager)
- Actian DataConnect Version 11 and prior versions
- Actian DataFlow

- Actian Ingres 11.0 and 11.1
- Actian Vector and VectorH 6.0

NOTE: Some on-premises products use Log4j 1.2.17, which is not vulnerable to CVE-2021-44228. We have done additional analysis on this fork and confirmed a new but similar vulnerability that can only be exploited by a trusted party. For that reason, Actian considers these to still be of 'low' impact.

Actian Products that do not use Log4j so are not impacted by this vulnerability:

- Actian Avalanche
- Actian Enterprise Access
- Actian FastObjects
- Actian OpenROAD
- Actian Zen

Actian Products that may have an indirect impact from this vulnerability. These Products do not ship/install with Log4j but provide an interface to use Log4J which the customer has to provide and has to explicitly enable/configure in the product.

- Actian NoSQL Database

For more information about Actian security alerts and to register to proactively receive these alerts by email, please register at the Actian Support Services site.

Should you have any further questions, please contact our Support Team.

Sincerely,

Pamela Fowler (she/her)
Senior VP, Customer Success
Actian | Support
M +1 708 415 2875
O +1 650 587 5504
actian.com

ACTIAN™
Powering the data-driven enterprise