Vulnerability Handling Policy

This policy supplements InterSystems Minimum Supported Version statement published at: https://www.intersystems.com/support/minimum-supported-version/ to clarify how security corrections are released and how customers can receive information about security issues in InterSystems IRIS® and InterSystems IRIS for Health™ (as well as InterSystems Caché®, and InterSystems Ensemble®).

Security Corrections

To release security corrections as soon as possible, actively supported maintenance releases (MRs) of InterSystems IRIS® contain security corrections along with performance and stability fixes. InterSystems provides regular MRs for the two most recent years of releases. InterSystems provides Extended Security Support (ESS) for one additional year, as well as for the latest release of InterSystems Caché® and InterSystems Ensemble®.

Under Extended Security Support, InterSystems evaluates security issues for the current and the **three** most recent years of InterSystems IRIS releases, as well as the latest maintenance release of Caché.

> *For example, in 2023, InterSystems will provide guidance related to security issues for InterSystems IRIS versions 2020.1.x, 2021.1.x, 2022.1.x, as well as the then current version 2023.1.x*

Additionally, InterSystems will provide fixes or mitigation guidance for Caché (version 2018.1.7 or whatever version supersedes it). InterSystems will provide security corrections for these releases and/or let customers know how to mitigate any potential security vulnerabilities in these releases.

Security corrections outside of this policy will be provided on a 'best effort' basis.

Supported Platforms

Supported Platforms are specified in the documentation of each release. For example, the supported platforms for the most recent version of InterSystems IRIS are listed at https://docs.intersystems.com/irislatest/csp/docbook/DocBook.UI.Page.cls?KEY=ISP_technologies.

Security patches are only provided for currently supported platforms as listed in the InterSystems product documentation. The minimum supported version of each of these platforms, unless explicitly specified otherwise, will be the latest maintenance release of the major release shown in these documents if that release is still supported by the vendor.

The information contained in this document is responsive to specific parameters relating to InterSystems products or services. This document is not intended as a general statement of character, sufficiency, quality, or composition of any process, product, service, or detail except as explicitly stated.

Security Notices

To notify customers of critical and high severity security issues, InterSystems provides security alerts. InterSystems publishes these alerts when a correction or mitigation is available for all supported releases—both MR and ESS releases—or when there is a risk of active exploitation of a vulnerability. This notification typically occurs after an ESS release is published with security fixes. Security corrections will be included in MRs before an ESS release is published.

InterSystems sends security alerts via email to the security contacts of registered customers. To add or update their security contacts, contact their InterSystems account manager. InterSystems strongly recommends that customers register an email alias for the security contacts instead of using named individuals.

Medium- and low-severity security corrections are published with MR and ESS releases in the release's change notes in the documentation, rather than as part of a security alert. For a medium-severity issue, MRs include a fix only if the change is unlikely to break existing applications; if there is a risk of breaking these applications, then the fix is ported to the next available Continuous Delivery (CD) release. (Also, if an ESS release does not include any critical- or high- severity corrections, then it is published without a corresponding security alert.)

Third-Party Components

InterSystems regularly updates third party components (TPCs) in each maintenance release. MR updates may include corrections for potential security vulnerabilities in these components. If InterSystems determines that a security issue reported in a TPC does not affect a release, it may not be updated.

If there is no risk to the stability of the release, InterSystems may update TPCs even when security issues are unlikely to result in an exploitable vulnerability.

Further Assistance

Technical Assistance from the Worldwide Response Center (https://wrc.intersystems.com) is available 24×7 for all versions, regardless of release date.

This is not a guarantee of future releases and is subject to change without notice.

The information contained in this document is responsive to specific parameters relating to InterSystems products or services. This document is not intended as a general statement of character, sufficiency, quality, or composition of any process, product, service, or detail except as explicitly stated.