

Azul Zulu builds of OpenJDK

November 2026 Monthly Update

Release Notes

Revision 1.0

Table of Contents

Revision History 1

Release Details 1

What's New 4

Monthly Critical Security Patch Updates 4

What to Expect from a CSPU 4

Dedicated Deserialization Filter for JMX RMI Connections 5

Transited Path Validation for Cross-Realm Kerberos Tickets 5

Configurable PATH Position in the Windows MSI Installer 5

IANA Time Zone Data Version 6

Supported Platforms 7

Azul Zulu Builds of OpenJDK Without and With OpenJFX 7

Azul Zulu Builds of OpenJDK With CRaC 11

Fixed Issues 13

Fixed Common Vulnerabilities and Exposures 13

Non-CVE Security Fixes 15

OpenJDK Fixes and Enhancements 15

OpenJFX Fixes and Enhancements 16

Fixes and Enhancements Specific to Azul Zulu Builds of OpenJDK 16

Fixes and Enhancements Specific to Azul Zulu Builds of OpenJDK With JavaFX . . . 17

Legal Notice 18

Revision History

Revision	Date	Description
0.1	November 17, 2026	Initial version of the document.
1.0	November 17, 2026	Added CVE information.

Release Details

This release is the November 2026 monthly update release (CSPU) for Azul Zulu Builds of OpenJDK version 27, 25, 21, 17, 11, 8, 7, and 6. Monthly updates were announced in the blog post Azul Will Deliver Monthly Java Critical Security Patch Updates, Increasing Patch Velocity with Stability.

The following table describes which Azul Zulu versions are published with this release.

Azul Zulu Version (*)	Update Type (**)	JDK Version	Based on		JavaFX Version
			Azul Zulu Version	JDK Version	
27.30.201 (CA) 27.30.202 (SA)	CSPU for **PSU**	27.0.1.1+4	27.30.110	27.0.1.0.3+1	27.0.1.1+200
25.37.202 (SA)	CSPU for **CPU**	25.0.4.1.201+1	25.37	25.0.4.1.103+1	25.0.4.0.201+201
25.38.201 (CA) 25.38.202 (SA)	CSPU for **PSU**	25.0.5.1+2	25.38.110	25.0.5.0.3+1	25.0.5.1+200
21.53.202 (SA)	CSPU for **CPU**	21.0.12.1.201+1	21.53	21.0.12.1.103+1	23.0.8.0.201+200
21.54.201 (CA) 21.54.202 (SA)	CSPU for **PSU**	21.0.13.1+2	21.54.110	21.0.13.0.3+1	23.0.9.1+200
17.69.204 (SA)	CSPU for **CPU**	17.0.20.1.201+1	17.69	17.0.20.1.103+1	22.0.10.0.201+200
17.70.201 (CA) 17.70.202 (SA)	CSPU for **PSU**	17.0.21.1+2	17.70.114	17.0.21.0.3+1	22.0.11.1+200

11.91.202 (SA)	CSPU for **CPU**	11.0.32.1.201+1	11.91	11.0.32.1.103+1	19.0.16.0.201+200
11.92.201 (CA) 11.92.202 (SA)	CSPU for **PSU**	11.0.33.1+1	11.92.114	11.0.33+10	19.0.17.1+200
8.97.0.202 (SA)	CSPU for **CPU**	8u513-b01	8.97	8u511-b103	8u513-b01
8.98.0.201 (CA) 8.98.0.202 (SA)	CSPU for **PSU**	8u514-b01	8.98.0.112	8u512-b09	8u514-b01
7.89.0.202 (SA)	CSPU for **CPU**	7u523-b01	7.89	7u521-b103	N/A
6.83.0.202 (SA)	CSPU for **CPU**	6b195	6.83	6b193	N/A

(*) Azul provides two types of distribution packages for each Java version:

- **Subscriber Availability (SA)** distributions are tested, certified, and commercially supported Azul Zulu Builds of OpenJDK. Azul ensures that the software that uses the Accessible APIs of the product doesn't have to include specific licenses and that such a use doesn't contaminate the code or intellectual property of such software with any license requirements. SA builds may support configurations and features that are unavailable to free users.
- **Community Availability (CA)** distributions are Azul Zulu Builds of OpenJDK that are free to download and use.

> **NOTE** Both SA and CA distributions may contain Early Access builds noted with `-ea-` in their filename. Early Access builds may not be TCK certified.

(**) Update type:

- **CSPU** (Critical Security Patch Update): Contains fixes to critical issues and security vulnerabilities, delivered on a monthly basis between regular quarterly update releases.

    - **CSPU for CPU**: Critical security patches applied to the latest quarterly CPU release.
    - **CSPU for PSU**: Critical security patches applied to the latest quarterly PSU release.
- **CPU** (Critical Patch Updates) contain fixes to security vulnerabilities and critical bug fixes. Azul Zulu CPU releases are generally based on prior-cycle PSU releases, with only security fixes applied. They provide a low-risk vehicle for the potentially urgent deployment of security fixes when issues of sufficient severity arise. CPU releases are available in SA distributions.
- **PSU** (Patch Set Updates) incorporates all fixes in the corresponding CPU, as well as additional non-security bug fixes. Azul Zulu PSU releases incorporate both security fixes and other changes that align the release contents with the associated OpenJDK project quarterly release. PSU releases are available in SA and CA distributions.

What's New

Monthly Critical Security Patch Updates

This is a monthly Critical Security Patch Update (CSPU) for Azul Zulu Builds of OpenJDK, based on the October 2026 quarterly update release. CSPUs close the gap between quarterly releases: as soon as a fix for a critical vulnerability becomes available for OpenJDK, it's delivered in the next monthly release window instead of waiting up to three months for the next quarterly release.

Like every quarterly update release, each CSPU comes with two sets of binaries: **CPU builds**, which contain only critical and security fixes, and **PSU builds**, which also accumulate non-security updates, aligned with OpenJDK from the previous release. If a CSPU carries security fixes that require an immediate reaction according to your company's security policy, you typically have less time to test before deploying. That's where the CPU binaries help: their minimal change set reduces the risk of regressions when validation time is short.

Each CSPU has its own release notes as it is not an addition to the release notes of the quarterly update release that precedes it.

What to Expect from a CSPU

The following points describe how CSPUs fit alongside the quarterly update releases:

- Quarterly update releases continue unchanged, in January, April, July, and October, on the third Tuesday of the month.
- A CSPU may be published in any month that has no quarterly update — that is, every month except January, April, July, and October. Like the quarterly releases, it lands on the third Tuesday of the month, following the OpenJDK release schedule.
- A CSPU is published only when critical security fixes warrant a monthly update release.
- Quarterly update releases remain cumulative and include every fix delivered in the preceding CSPUs (if any).

- A CSPU covers the same Azul Zulu versions, release configurations, package types, Linux package repositories, and container images as a quarterly update release, and is delivered under the same support SLA.

To handle a CSPU in your patch process, treat it exactly as you treat a quarterly update release: pull it into dependency management, run your existing test suite, and promote it through your normal pipeline.

Dedicated Deserialization Filter for JMX RMI Connections

The JMX RMI connector now deserializes encoded `JMXServiceURL` stubs (`service:jmx:rmi:///stub/…`) with a dedicated filter. The filter is built from the connector environment property and the system property `jmx.remote.rmi.connector.url.filter.pattern`, which are checked in that order. Both use the same syntax as `jdk.serialFilter`.

This filter replaces `jdk.serialFilter` for this deserialization. A class that doesn't match any rule in the filter is only accepted if it implements `RMIClientSocketFactory` or `RMIServer`; otherwise it's rejected.

Transited Path Validation for Cross-Realm Kerberos Tickets

The Kerberos acceptor now validates the transited path of cross-realm tickets. It checks the transited realms against the `[capaths]` section of `krb5.conf`, or against the realm name hierarchy if `[capaths]` is not configured. Tickets with a path that is not allowed are rejected with `KRB_AP_PATH_NOT_ACCEPTED`.

The new system property `sun.security.krb5.acceptor.checkTransitedPolicy` controls this check. Its default is `true`. Set it to `false` to restore the previous behavior.

Configurable PATH Position in the Windows MSI Installer

The Azul Zulu MSI installer now lets you choose where `<INSTALLDIR>\bin` is added to the `PATH` environment variable. By default, it's still added to the beginning. To add it to the end instead, for example to avoid precedence over system directories when

installing in a custom folder, select the new **Add to the end of PATH** check box or set `ADD_TO_END_OF_PATH=1` on the command line.

For details, including upgrade behavior, see path-position in the Windows installation instructions.

IANA Time Zone Data Version

This release of Azul Zulu comes with IANA Time Zone Database version **tzdata2026f**.

Supported Platforms

This section provides information about the operating systems that are supported in this release of Azul Zulu.

Azul Zulu Builds of OpenJDK Without and With OpenJFX

Some versions of Azul Zulu are available in different packages for specific platforms, as indicated in this overview table with:

- ✔ : Build of OpenJDK without OpenJFX.
- ✔✔: Build of OpenJDK without and with OpenJFX.

> **NOTE**
>
> The list of supported configurations and platform includes, but is not limited to, the table below. Don't hesitate to contact Support if you have issues with Azul Zulu Builds of OpenJDK on any other platform or configuration.

Operating System	Azul Zulu Version							
	6	7	8	11	17	21	25	27
Windows (x86 32/64-bit)								
Windows Server 2025	✔	✔	✔✔	✔✔	✔✔	✔✔ [1]	✔✔ [1]	✔✔ [1]
Windows Server 2022	✔	✔	✔✔	✔✔	✔✔	✔✔ [1]	✔✔ [1]	✔✔ [1]
Windows Server 2019	✔	✔	✔✔	✔✔	✔✔	✔✔ [1]	✔✔ [1]	✔✔ [1]
Windows Server 2016	✔	✔	✔✔	✔✔	✔✔	✔✔ [1]	✔✔ [1]	✔✔ [1]
Windows 11	✔	✔	✔✔	✔✔	✔✔	✔✔ [1]	✔✔ [1]	✔✔ [1]
Windows (ARM 64-bit)								

Windows 11	n/a	n/a	n/a	n/a	✔	✔	✔	✔
Linux (x86 32/64-bit)								
RHEL 10.x [2]	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
RHEL 9.x	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
RHEL 8.x	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
RHEL 7.x	n/a	n/a	✔	✔	✔	n/a	n/a	n/a
Fedora 44	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
SLES 16	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
SLES 15	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
SLES 12	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
CentOS Stream 9	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
Ubuntu 26.04	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
Ubuntu 24.04	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
Ubuntu 22.04	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
Debian 13	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
Debian 12	✔	✔	✔	✔	✔	✔ [1]	✔ [1]	✔ [1]
Wind River 8.x	n/a	✔	✔	n/a	n/a	n/a	n/a	n/a

Alpine Linux 3.24	n/a	n/a	✔	✔	✔	✔	✔ [1]	✔ [1]
Wolfi Linux	n/a	n/a	n/a	n/a	n/a	✔	✔	✔ [1]
Amazon Linux 2023	n/a	n/a	✔	✔	✔	✔	✔ [1]	✔ [1]
Linux (ARM 64-bit)								
Ubuntu 26.04	n/a	n/a	✔✔	✔✔	✔✔	✔✔	✔✔	✔✔
Ubuntu 24.04	n/a	n/a	✔✔	✔✔	✔✔	✔✔	✔✔	✔✔
Ubuntu 22.04	n/a	n/a	✔✔	✔✔	✔✔	✔✔	✔✔	✔✔
Debian 13	n/a	n/a	✔✔	✔✔	✔✔	✔✔	✔✔	✔✔
Debian 12	n/a	n/a	✔✔	✔✔	✔✔	✔✔	✔✔	✔✔
Alpine Linux 3.24	n/a	n/a	✔	✔	✔	✔	✔	✔
Wolfi Linux	n/a	n/a	n/a	n/a	n/a	✔	✔	✔
Amazon Linux 2023	n/a	n/a	✔	✔	✔	✔	✔	✔
Linux with kernel 3.10.x and glibc 2.23 [3] [4]	n/a	n/a	✔	✔	n/a	n/a	n/a	n/a
Linux (ARM 32-bit Hard-Float)								
Ubuntu 18.04 [5]	n/a	n/a	✔	✔	✔	✔ [6]	✔ [6]	n/a
Raspberry Pi OS 10 (Buster) [5]	n/a	n/a	✔	✔	✔ [7]	✔ [7] [6]	✔ [7] [6]	n/a
Raspberry Pi OS 9 (Stretch) [5]	n/a	n/a	✔	✔	n/a	✔ [7] [6]	✔ [7] [6]	n/a
Linux with kernel 3.10.x and glibc 2.9 [5] [8]	n/a	n/a	✔	✔	n/a	✔ [6]	✔ [6]	n/a
Linux (ARM 32-bit Soft-Float) [9]								

Linux with kernel 2.6.34 and glibc 2.5 [10]	n/a	n/a	✔	✔	n/a	n/a	n/a	n/a
Debian 7 Wheezy [11]	n/a	n/a	✔	✔	n/a	n/a	n/a	n/a
Linux with kernel 3.10.x and glibc 2.9 [11]	n/a	n/a	✔	✔	n/a	n/a	n/a	n/a
Linux (MIPS 32-bit) [12]								
Linux with kernel 4.9.59 and glibc 2.9 [13]	n/a	n/a	✔	n/a	n/a	n/a	n/a	n/a
Linux (ppc64 Big Endian)								
Linux with kernel 3.8.13 and glibc 2.22 [14]	n/a	n/a	✔	n/a	n/a	n/a	n/a	n/a
Linux (ppc32 Hard-float and SPE)								
Linux with kernel 3.12.37 and glibc 2.20 [15]	n/a	n/a	✔	n/a	n/a	n/a	n/a	n/a
QNX								
QNX 7.0 ARMv7 32-bit Hard-Float ABI	n/a	n/a	✔	n/a	n/a	n/a	n/a	n/a
QNX 7.1 ARMv8 32-bit Hard-Float ABI	n/a	n/a	✔	n/a	n/a	n/a	n/a	n/a
macOS (x86 64-bit)								
macOS 15+	n/a	✔	✔	✔	✔	✔	✔	✔
macOS (Apple Silicon)								
macOS 15+	n/a	n/a	✔	✔	✔	✔	✔	✔
Solaris (x86 and Sparc)								
Solaris 11	n/a	✔	✔	✔	n/a	n/a	n/a	n/a
Solaris 10	n/a	✔	✔	n/a	n/a	n/a	n/a	n/a

1. Build of OpenJDK (with and without OpenJFX) only for 64-bit.

2. Only available in PSU builds

3. Bundles with the Checkpoint/Restore (with the `criu` suffix) functionality require kernel 4.4.0+.
4. Bundles compiled with GCC 9 (with the `gcc9` suffix) require glibc 2.29.
5. Bundles with the C1 compiler were tested on ARMv6/ARMv7/ARMv8 hardware. Bundles with both C1 and C2 compilers were tested on ARMv7/ARMv8 hardware.
6. This bundle is only available as a Subscriber Availability (SA) distribution.
7. Linux (ARM 32-bit Hard-Float) Zulu 17+ is only supported on Raspberry Pi boards with an ARMv7 or ARMv8 processor and can't be used on, e.g., Raspberry Pi 1 and Raspberry Pi Zero 1.
8. Bundles with the CRaM (with the `cr` suffix) functionality require glibc 2.13.
9. Bundles with the C1 compiler use FPU, if it is present and available, to speed up floating point operations. Bundles with both C1 and C2 compilers require FPU.
10. Bundles with the C1 compiler. Tested on ARMv5 hardware.
11. Bundles with the C1 compiler were tested on ARMv6 and ARMv7 hardware. Bundles with both C1 and C2 compilers were tested on ARMv7 hardware.
12. MIPS32r2 ISA, Big Endian, FPU in 32-bit mode or equivalent emulation.
13. Linux soft-float O32 MIPS ABI.
14. Bundles for this platform were tested on QorIQ® T4240-RDB.
15. Hard-Float EABI bundles were tested on QorIQ® T1024RDB. SPE ABI bundles were tested on NXP® P2020RDB.

Azul Zulu Builds of OpenJDK With CRaC

NOTE

Currently, CRaC is only available for the specified Linux systems, in the versions listed below of Azul Zulu Builds of OpenJDK. For development, you can use the CRaC Java library on any platform and simulate the CRaC functionality.

- ✔️ : Build of OpenJDK with full CRaC support and the Warp engine.
- ✔️ : Build of OpenJDK with CRaC support for development purposes. These provide a simulated checkpoint/restore mechanism to be used for development and testing.

Operating System	Azul Zulu Versions	
	17, 21, 25, 27	
	x86 64-bit	ARM 64-bit
Linux	✔	✔
Alpine Linux 3.24	✔	✔
Windows	✔	n/a
macOS	✔	✔

Fixed Issues

This section covers all issues that were fixed in this release.

Fixed Common Vulnerabilities and Exposures

This section summarizes Common Vulnerabilities and Exposures (CVE) fixed in this release.

No.	CVE #	Component	Protocol	Remote Exploit w/o Auth.	Base Score	Attack Vector	Attack Complex	Privileges Req'd	User Interact	Scope	Confiden-tiality	Integrity	Availability	Azul Zulu Versions Affected	Notes
1	CVE-2026-114938	Compiler	Multiple	Yes	8.1	Network	High	None	None	Unchanged	High	High	High	27, 25, 21, 17	Note 1
2	CVE-2026-86144	JavaFX (libxml2)	Multiple	Yes	7.5	Network	High	None	Required	Unchanged	High	High	High	27, 25, 21, 17, 11, 8	Note 2
3	CVE-2026-114939	JGSS	Multiple	Yes	7.4	Network	High	None	None	Unchanged	High	High	None	27, 25, 21, 17, 11, 8, 7, 6	Note 2
4	CVE-2026-114940	JSSE	TLS	Yes	7.4	Network	High	None	None	Unchanged	High	High	None	27, 25, 21, 17, 11, 8	Note 3
5	CVE-2026-114941	Compiler	Multiple	Yes	7.0	Network	High	None	None	Unchanged	Low	Low	High	27, 25, 21	Note 1
6	CVE-2026-114942	Libraries	Multiple	Yes	7.0	Network	High	None	None	Unchanged	Low	Low	High	27, 25, 21, 17	Note 1
7	CVE-2026-114943	Hotspot	Multiple	Yes	6.5	Network	High	None	None	Unchanged	None	Low	High	27, 25, 21, 17, 11, 8	Note 3
8	CVE-2026-114944	Core Java Libraries	Multiple	Yes	5.9	Network	High	None	None	Unchanged	None	High	None	27, 25, 21, 17, 11, 8, 7, 6	Note 3
9	CVE-2026-114945	Libraries	Multiple	Yes	5.3	Network	Low	None	None	Unchanged	None	Low	None	27, 25, 21, 17	Note 3

No.	CVE #	Component	Protocol	Remote Exploit w/o Auth.	Base Score	Attack Vector	Attack Complex	Privileges Req'd	User Interact	Scope	Confiden-tiality	Integrity	Availability	Azul Zulu Versions Affected	Notes
10	CVE-2026-114946	Compiler	Multiple	Yes	4.8	Network	High	None	None	Unchanged	Low	Low	None	27, 25, 21, 17, 11, 8, 7, 6	Note 3
11	CVE-2026-114947	JSSE	TLS	Yes	3.7	Network	High	None	None	Unchanged	None	Low	None	27, 25	Note 2

Notes:

ID	Notes
1	This vulnerability can only be exploited by supplying data to APIs in the specified Component, such as through a web service.
2	This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
3	This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.

Non-CVE Security Fixes

The following table summarizes non-CVE security fixes implemented in this release.

OpenJDK Patch ID	Azul Zulu Version	Synopsis	CPU/PSU
No issues fixed in this release			

OpenJDK Fixes and Enhancements

The following table describes the OpenJDK changes implemented in this release.

OpenJDK Patch ID	Azul Zulu Version	Synopsis	CPU/PSU
JDK-8274205	7	Handle KDC_ERR_SVC_UNAVAILABLE error code from KDC	CPU,PSU
JDK-8316771	7,8,11,17,21	Krb5.java has not defined messages for all error codes	CPU,PSU
JDK-8396048	6,7,8,11,17,21,25,27	(tz) Update to tzdata2026f	CPU,PSU
JDK-8384495	8	Update Libpng to 1.6.58	PSU
JDK-8392979	27	Update the Nov CPU26_11 release date to the newly created stabilization branches	PSU
JDK-8393195	8,11,17,21,25,27	Update Libpng to 1.6.59	PSU
JDK-8394492	8,11,17,21,25,27	Update FreeType to 2.15.0	PSU
JDK-8394581	17	[17u] TestSHA512Intrinsics.java and TestSHA512MultiBlockIntrinsics.java fail with JDK 17 on Graviton Hosts	PSU
JDK-8394663	25	Bump update version for OpenJDK: jdk-25.0.5.1	PSU
JDK-8394664	21	Bump update version for OpenJDK: jdk-21.0.13.1	PSU
JDK-8394665	17	Bump update version for OpenJDK: jdk-17.0.21.1	PSU

OpenJFX Fixes and Enhancements

The following table describes the JavaFX changes implemented in this release.

OpenJDK Patch ID	Azul Zulu Version	Synopsis	CPU/PSU
JDK-8392009	8,11,17,21,25, 27	Update libxml2 to 2.15.4	CPU,PSU

Fixes and Enhancements Specific to Azul Zulu Builds of OpenJDK

The following table describes the Azul Zulu changes implemented in this release.

Issue ID	Azul Zulu Version	Synopsis	CPU/PSU
ZULU-102341	25	Update PQJSSE for Nov CSPU	CPU,PSU
ZULU-102386	25	Update JFX to zulu25.0.4.0.201+201	CPU,PSU
ZULU-102535	21	Update JFX to zulu23.0.8.0.201+200	CPU,PSU
ZULU-102536	17	Update JFX to zulu22.0.10.0.201+200	CPU,PSU
ZULU-102562	11	Update JFX to zulu19.0.16.0.201+200	CPU,PSU
ZULU-102572	8	Update JFX to zulu8u513-b01	CPU,PSU
ZULU-101509	11,17,21,25	32-bit builds fail after JDK-8394492	PSU
ZULU-102569	27	Update JFX to zulu27.0.1.1+200	PSU
ZULU-102667	25	Update JFX to zulu25.0.5.1+200	PSU
ZULU-102668	17	Update JFX to zulu22.0.11.1+200	PSU
ZULU-102669	11	Update JFX to zulu19.0.17.1+200	PSU
ZULU-102678	21	Update JFX to zulu23.0.9.1+200	PSU
ZULU-102682	8	Update JFX to zulu8u514-b01	PSU

Fixes and Enhancements Specific to Azul Zulu Builds of OpenJDK With JavaFX

The following table describes the Azul Zulu changes implemented in this release.

Issue ID	Azul Zulu Version	Synopsis	CPU/PSU
ZULU-92098	8,11,17,21,25,27	Add Nexus GitHub proxy support for ICU and libAV repositories in JFX build	CPU,PSU
ZULU-101497	8,11,17,21,25,27	Get ffmpeg sources from github instead of ffmpeg.org	CPU,PSU
ZULU-101434	8	Zulu FX 8: JavaFX MediaPlayer H.264 MP4 fails with ERROR_MEDIA_INVALID from 8u502 (last good 8u492)	PSU

Legal Notice

© 2005–2026, Azul Systems, Incorporated, 375 Moffett Park Drive, Suite 115, Sunnyvale, CA 94089. All rights reserved.

Products and specifications discussed in this document may reflect future versions and are subject to change without notice. Azul Systems assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Azul Systems. Please note that the content in this document is protected under copyright law even if it is not distributed with software that includes an end user license agreement.

Azul Systems, Azul Zulu, and the Azul logo are trademarks or registered trademarks of Azul Systems, Inc. Linux is a registered trademark of Linus Torvalds. Java is a registered trademark of Oracle Corporation. Microsoft and Windows are registered trademarks of Microsoft Corporation. Other marks are the property of their respective owners and are used here only for identification purposes.