

System Integrity

Protect enterprise compliance and remain vigilant against threats

What is System Integrity?

The IBM® System Integrity Statement represents decades of confidence and commitment in the [IBM Z®](#) and [IBM LinuxONE](#) platforms. System integrity has many facets, including excellence in [system security](#), design and development. These are all intended to prevent unauthorized application programs, subsystems and users from bypassing system security, preventing them from gaining access, circumventing, disabling, altering or obtaining control of key system processes and resources unless allowed by the installation.

[Explore](#)  [z/OS security videos](#)

Our commitment to System Integrity

In the event of an IBM system integrity or security vulnerability issue is reported, IBM will always take action to investigate, and if validated, take appropriate action to resolve it.

These actions may include development of fixes, identification of applicable workarounds, recommending migration to a later release and more.

System Integrity is the inability of any program not authorized by a mechanism under the installation's control to circumvent or disable store or fetch protection, access a resource protected by a Security Server/Manager, or obtain control in an authorized state; that is, in supervisor state, with a protection key less than eight (8), or Authorized Program Facility (APF) authorized.

A **security vulnerability** is a set of conditions in the design, implementation, operation or management of a product or service that is unable to prevent an attack, resulting in exploitations such as controlling or disrupting operation, compromising (i.e. deleting, altering or extracting) data, or assuming ungranted trust or identity. Examples range from TCP/IP or Java™ architectural concerns to things like Denial of Service (DoS) attacks, heuristic or algorithm errors and more.

System Integrity statements by operating system

IBM z/OS®

The protection of your system, transactions, data and applications from accidental or malicious modification is one reason IBM Z is the trusted platform.

 [View z/OS Statement \(77 KB\)](#)

IBM z/VM®

IBM is committed to the System Integrity of the z/VM environment – helping customers get the best protection for their data.

 [View z/VM Statement](#)

IBM z/TPF and z/VSE®

Clients should obtain the latest service information, including security and system integrity APARs, from the Service and Support site.

[View z/TPF Service and Support](#)

[View z/VSE Service and Support](#)

Note: Security information and updates for the Linux operating system, running on either IBM Z or IBM LinuxONE should be obtained directly from the Linux distribution partners.

Register for access to the IBM Z and LinuxONE Security Portal

IBM utilizes internal and external sources to uncover potential vulnerabilities. IBM Z offers a Security Portal that allows clients to stay informed about patch data, associated Common Vulnerability Scoring System (CVSS) ratings for new APARs and Security Notices to address highly publicized security concerns.

How to register

To register, you will need to provide your company name, your name and your ResourceLink or [IBMid](#). IBM will verify that you are an IBM Z or LinuxONE customer or an authorized representative.

[Register now](#)

Who should register

If you are an IBM Z or LinuxONE customer or an authorized representative, register to access the IBM Z or LinuxONE Security Portal for IBM Z Security/Integrity APAR information for z/OS and z/VM as well as security updates that pertain to hardware/firmware.

Terms and Conditions

By accessing the IBM Z and LinuxONE Security Portal, you agree the information contained in it is IBM Confidential, provided AS IS, may be used by you for internal purposes only and may not be disclosed to any third party without IBM's prior written consent.

If you do not agree to these conditions, you may not access the IBM Z and LinuxONE Security Portal. Please ensure that you update all of your IBM Z products to a supported version. Security and integrity fixes are generally only issued for supported versions of IBM Z products.

Note: All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice. Any reliance on this Statement of Direction is at the relying party's sole risk and will not create any liability or obligation for IBM.