IBM Z
Introduction
July 2018

IBM Z Security Portal

Frequently Asked Questions

Worldwide

ZSQ03054-USEN-05

IBM Z Security Portal

What is the origin of the IBM Z® Security Portal?

The current Security Portal began as a beta project with several of our most security conscious clients leading the direction of the program with their requirements and insight. We jointly created content and a process that met the needs (operational, regulatory, etc.) of the clients while minimizing their security risk. Since then we have made major improvements and updates to the Security Portal based on continued client feedback and Design Thinking engagements. We meet with our IBM Z clients regularly to provide educational updates and to gather requirements. We engage with clients as needed to assist in the integration of the Security Portal in their enterprise security process and policy.

How do I gain access to the IBM Z Security Portal?

The instructions for access to the IBM Z Security Portal can be found at
https://www.ibm.com/it-infrastructure/z/capabilities/system-integrity

What is provided on the IBM Z Security Portal?

The IBM Z Security Portal currently has Security / Integrity APAR information for the z/OS® and z/VM® operating systems and associated IBM products along with critical Security Notices that address hardware, firmware and software issues. Security information for the z/TPF operating systems is now included in the Security Notice section.

How do I gain authorization to the IBM Z Security Portal?

Authorization is granted to the IBM Z Security Portal once a client has completed the registration process. To meet the requirements of our clients this process ensures that only the correct individuals that have a need to know in the client's organization can gain access to the information they need to properly maintain their IBM Z environments.

What is the difference between being authorized and subscribed to the IBM Z Security Portal?

Once a client is authorized you have the option to subscribe to the IBM Z Security Portal to receive notifications via email. IBM strongly recommends you subscribe. The notification will let you know when information is added and if any existing record is updated. This means if any cumulative files or notices are updated the subscriber will get an email notifying them what has been updated. No sensitive information is provided via email. If a client chooses not to subscribe, they must be vigilant in checking for new posts to the Security Portal on a regular basis.

I am having trouble locating the latest information in the IBM Z Security formation that is relevant to my enterprise role. How can I better navigate the Security Portal?

As the Security Portal has grown over time the volume and type of data that is provided has expanded. We continue to work closely with clients to help provide a portal experience that meets their needs. The Security Portal has a new look and feel with the use of category tabs, enhanced search, sort and filter capabilities. The Security Portal landing page now has three tabs (Primary resources, Security notices, and APARs) to better direct your query based on your role. The Primary resources tab is where you will find the Enhanced HOLDDATA, Common Vulnerability Scoring System (CVSS) and Security Integrity APAR (SIA) cross reference files [discussed later in this document]. The Security Notice and APAR tabs provide greater detail and now have the ability to sort on data or number and filter on key terms like z/OS,

z/VM, WebSphere®, etc. to help get you to the information you need faster. The Search capability has also been refined to better highlight content within the Resource Link site.

How does the SECINT Enhanced HOLDDATA compare with Enhanced HOLDDATA from other sources?

Clients can only get Security / Integrity (SECINT) HOLDDATA for z/OS from the IBM Z Security Portal. Non-Security related Enhanced HOLDDATA can be downloaded separately from another source (http://service.software.ibm.com/holdata/390holddata.html). Together, using SMP/E, these two sources can help provide a complete picture of what updates are available for a given system.

How is SECINT Enhanced HOLDDATA used?

For z/OS the Security Portal provides enhanced HOLDDATA for Security / Integrity APARs. This data is used as input to SMP/E along with the generally available non-Security / Integrity HOLDDATA. Together, these two files will be used as input to SMP/E and will provide a report for the IBM Z infrastructure team. Clients can use this data to help ensure their various IBM Z environments are up to date and they know what APARs need to be installed to keep the system up to date with regard to service.

Why is this Security Portal necessary?

IBM does not make Security / Integrity data publicly available for IBM Z. This Security Portal provides a controlled notification and distribution mechanism to help ensure this critical information is available only to those IBM Z clients that have a need to know without publicly posting information that could put their systems in danger.

Why are Security / Integrity APARs not publicly posted via CERT vulnerabilities, CVE or other means?

Working closely with IBM Z clients over the years continues to support the position that, Security / Integrity APAR data should be kept confidential and provided to only those that have a verifiable need to know. Organizations, like US-CERT and CVE as well as have a different philosophy. They believe in full disclosure and the public dissemination of vulnerability information. There are pros and cons to each approach and we, along with many mainframe customers, believe that public release of this data is not in the best interest of the IBM Z community. Since IBM provides both the operating system and the hardware under licensing agreements it is relatively easy to verify each client has access to the security information they need to keep their systems up to date.

Why are CVE or CERT VU numbers not incorporated in the APAR information provided to clients?

In conjunction with client requirements, IBM Z supports the policy to ensure that the details of Security / Integrity APARs not be made publicly available. In some cased these details might have been reported by a particular client and reporting details could put their enterprise at risk. Adding a CVE or CERT VU number to an APAR description would provide additional detail that could increase risk to clients. In the case of a highly publicized vulnerability there may be a Security Notice added to the Security Portal that may contain both CVE information and possible mitigations to help reduce risk to well-known issues. It is critical that both APAR information and Security Notices are both monitored regularly in accordance with your security policy.

Who needs access to the IBM Z Security Portal?

IBM strongly recommends that every IBM Z client subscribe to the Security Portal. However, each client needs to review their security policy and evaluate how best to integrate IBM Z security patch management into their enterprise security strategy.

How can I derive value from the IBM Z Security Portal?

The initial value of this site is in the aggregated list of security and system integrity APARs for both z/OS and z/VM. You will find this list if you search on the "Security Alerts" page for "z/OS Security / Integrity Data" or "z/VM Security / Integrity Data". For z/OS this is the HOLDDATA for the Security and Integrity APARs that is used as input for SMP/E. The z/VM file is a human readable file that contains the relevant APAR and PTF information for security and system integrity issues. At a minimum these security fixes should be applied. Security Notices are an added value, providing critical information and insight on a platform wide array of topics.

What information is provided in the z/OS CVSS data file?

This file contains an aggregated list of security and system integrity APARs for z/OS. It contains CVSS information that can be used to help determine the urgency and applicability of a security fix to your system. Specifically, it includes for each Security / Integrity APAR the associated base and temporal CVSS Base and Temporal scores to help determine the urgency and the CVSS Vector to address the applicability to your environment based on mitigating factors, workload, impact to the business, etc.

For more information on this security fix data, see this introductory video.

More information about CVSS scores and the CVSS Vector can be found in this FAQ and on the FIRST web site (http://www.first.org/cvss/).

What information is provided in a z/OS HOLDDATA record?

In this record you will find the applicable z/OS FMID, and the security or integrity APAR number included after the REASON keyword. In the COMMENT you will find the PTF number follows the FIX keyword and when applicable the CVSS base and temporal score might follow the SYMP keyword. If you are curious about the date of an APAR in the HOLDDATA records there is a DATE (YYJJJ) field where YY = the last two digits of the year and JJJ is the Julian date of the last update to the record.

How can I view the files attached to the various records in the IBM Z Security Portal?

The most important records in the IBM Z Security Portal contain files that are updated on a regular basis as necessary. Some of these files, like the CVSS and z/VM data, are intended to be read by humans, while the z/OS HOLDDATA file is intended for computer processing. Files, such as "*date* secint.holds", "*date* secint.cvss" or "*date* vvinteg.txt", are all plain text files that can be viewed on any platform that can view a plain text ASCII file. They were intentionally created as plain text to eliminate any requirement on a particular hardware platform or software product. If the files are difficult to read due to the formatting of columns use a fixed width (non-proportional) font such as "courier" for viewing.

How can I rate or prioritize IBM Z APARs for installation in my enterprise?

We have adopted the use of the CVSS (Common Vulnerability Scoring System) to help clients better understand the nature and relative criticality of APARs. Further information about CVSS and a guide to scoring can be found on the FIRST (Forum of Incident Response and Security Teams) web site (http://www.first.org/cvss/). A Base and Temporal score are provided. If an Environmental score is

required this must be computed by the client using the provided CVSS vector, taking into consideration their enterprise environment and a system by system evaluation.

What version of CVSS is used in the Security Portal?

When the IBM Z Security Portal became available, CVSS version 2 (V2) was in common use. If no version number is specified in the CVSS Vector string that Base score and Vector is derived using CVSS V2. When the version 3 (V3) specification was introduced by FIRST, the "CVSS:3.0" prefix was added to the Vector string to differentiate between V2, V3.0 and future versions of the CVSS specification. See the following for examples of CVSS Vectors:

Sample CVSS V2 Vector: (AV:L/AC:L/Au:N/C:P/I:N/A:N)

Sample CVSS V3 Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L)

How is the information obtained via the Security Portal related to the PMR process?

The PMR process is unchanged. This remains the mechanism for clients to report problems to IBM. A problem may or may not be a security or integrity concern. If a problem is determined to be a security or integrity vulnerability the resulting APAR/PTF will be treated as IBM Confidential and subsequently available via the IBM Z Security Portal. For PMRs opened for information about security or integrity APARs/PTFs, customers will be directed to the Security Portal.

Are the fixes for the Security / Integrity information found in the IBM Z Security Portal included in the RSU?

Yes, the Security / Integrity fixes are also included in the RSU on the same schedule as other critical service, such as PE and HIPER fixes. Using the Security Portal, however, gives you a chance to see the Security / Integrity APARs once they are closed and assess the risk early (using the new CVSS data). There may be some that you might determine need to be applied before the RSU is available. Our goal is to help ensure you have the data as soon as possible to make the best decisions for your enterprise.

Why do different platforms have different processes for disclosing vulnerability information?

Some platforms have chosen to publicly disclose their security vulnerability information. For these platforms this method makes sense. For example, a Linux® distribution does not know every machine, in every country, that is running a particular version of Linux. Given the number of Linux images in the world they cannot risk that an unpatched security vulnerability might permit malicious users to take over these machines and use them in a disruptive or surreptitious manner.

The IBM Z platform is different. It is a much smaller audience that is well known. Both the z/OS and z/VM operating systems are licensed products that make each valid customer known to IBM. With the critical workloads running on these systems, the impact of a vulnerability being exploited, however, could severely damage customer operations and business. IBM Z customers can gain access to the IBM Z Security Portal with the confidence that IBM attempts to limit access to IBM Z clients and thus exclude malicious users.

Why are the details of a vulnerability not publicly available?

One of the benefits for not providing vulnerability details is that both external attackers and internal personnel threats cannot get access to information that could put an enterprise at undue risk. Efforts to

limit the attack surface by limiting information to those who demonstrate a need to know will continue to help to mitigate enterprise vulnerability to attacks.

How can I assess the risk associated with a particular APAR?

At times clients have asked IBM to rank APARs as high, medium or low severity, to help them assess the risk of a given APAR. This has always been a concern since IBM Z has such a vast and diverse set of customers and workloads. We could not envision ranking an exposure in a way that was meaningful to all customers, workloads or enterprise environments. After evaluating this requirement further, it became evident that using the Common Vulnerability Scoring System (CVSS) would give our clients the data they needed to better evaluate the risk of an APAR with regard to their individual system and workload needs while still maintaining the confidentiality of the vulnerability details. Each APAR is assigned a CVSS Base score and Vector. The Base score is used to get a preliminary idea of the urgency of the APAR while the Vector is used to better understand the applicability of the APAR to a particular enterprise environment.

How can I use the CVSS Vector to better understand how an APAR or fix might apply to my Z environment?

The CVSS Vector contains information or metrics that capture the characteristics of the potential vulnerability. These metrics include, but are not limited to, the access vector, attack complexity and a measure of impact to confidentiality, integrity and availability to a vulnerable system. Depending on the workload and or other security measures, process or policies in place these metrics may indicate there is more or less risk.

The following table is provided for demonstration purposes only and does not replace the detailed explanations provided by FIRST (Forum of Incident Response and Security Teams) in their CVSS specification documents. One means for determining the applicability of a vulnerability might be to better understand the workload on that system and what impact metrics are critical to the service level agreement (SLA). Visualizing the vulnerability with colors might help identify the “hot” spots that attributed to the Base score. Using the following chart we will consider the impact of each metric using the associated color on a few example CVSS Vectors.

CVSS Version 2 Metric		Values		
		Bad	Worse	Worst
AV	Access Vector	**L**ocal	**A**djacent Network	**N**etwork
AC	Access Complexity	**H**igh	**M**edium	**L**ow
Au	Authentication	**M**ultiple	**S**ingle	**N**one
C	Confidentiality Impact	**N**one	**P**artial	**C**omplete
I	Integrity Impact	**N**one	**P**artial	**C**omplete
A	Availability Impact	**N**one	**P**artial	**C**omplete

Examples:

Base Score	Vector
7.2	(AV:L/AC:L/Au:N/C:C/I:C/A:C)
3.6	(AV:L/AC:L/Au:N/C:P/I:P/A:N)
5.8	(AV:N/AC:M/Au:N/C:P/I:P/A:N)

In the first example, you can see how the complete impact on confidentiality, integrity and availability impacts the score in contrast to it being a local attack vector. On the other hand, we see in the last

example that a partial impact to confidentiality and integrity may be more critical since this is a network attack. Each vector helps in the evaluation of the applicability and can only be fully understood when the systems, their workloads and other mitigating security measures are considered.

Please note the above table and examples use CVSS Version 2 for simplicity. The CVSS data in the Security Portal may be version 2 or version 3 depending on the origin and time frame of the vulnerability.

I noticed a new cross reference file that contains an SIA number. Who is this for and what is an SIA number?

A Security Integrity APAR (SIA) number is a number that is generated and used to communicate with clients that have a contract with IBM to manage their IBM Z environments. The SIA number is a way of identifying a Security or System Integrity APAR in a client's change management system without disclosing any IBM confidential APAR information. IBM has no control over who might have access to a client owned change management system or how they might propagate that data and IBM must protect all APAR information to minimize risk for all IBM Z clients. The client personnel that have demonstrated a need to know must be vetted through the normal process to gain access to the IBM Z Security Portal, agreeing to the terms and conditions of the portal. In the portal they can view the cross-reference file and gain access to the rest of the customer accessible APAR information.

We recognize that the information contained in the IBM Z Security Portal is IBM confidential and as a condition to our being granted access to the portal, we have agreed to terms and conditions presented on the portal that, among other things, prohibits our sharing such information with third parties. My company has hired an outside auditor who in the course of performing their audit requires access to my company's books, records, and systems in order that they may render an opinion. Would this auditor be considered a third party and can I give them access to IBM's confidential information on or from the portal?

The auditor would be a third party and absent IBM's consent you may not disclose to them IBM confidential information.

How can I obtain IBM's consent to share information with a third party?

You must send an email to IBM at syszsec@us.ibm.com requesting consent to disclose IBM confidential information to a third-party auditor. In your email, you must acknowledge the confidentiality terms under which you have been granted access to the Security Portal, identify the auditor and the specific IBM confidential information you seek to disclose. In addition, you must confirm in writing that you have entered into a written agreement with the auditor sufficient to require that the auditor treats the IBM confidential information in accordance with the terms and conditions on the Security Portal, including the nondisclosure obligations. IBM will consider your request, and in its sole discretion will decide whether to provide you such consent.

My company is an IBM Z customer as well as a services provider to others. We provide information technology (IT) services to many other companies that do not have access to the IBM Z Security Portal and therefore have not accepted the terms and conditions on the IBM Z Security Portal. Some of our customers are required by regulations to audit our security policies and practices as their IT services provider. How can we proceed with this audit and provide them with the information they need?

You must send an email to IBM at syszsec@us.ibm.com requesting consent to disclose IBM confidential information to a third-party auditor or your customer. In your email, you must acknowledge the confidentiality terms under which you have been granted access to the Security Portal, identify the auditor/customer and the specific IBM confidential information you seek to disclose. In addition, you must confirm in writing that you have entered into a written agreement with the auditor/customer sufficient to require that the auditor/customer treats the IBM confidential information in accordance with the terms and conditions on the Security Portal, including the nondisclosure obligations. IBM will consider your request, and in its sole discretion will decide whether to provide you such consent.

What are Security Notices and how do they differ from the HOLDATA and CVSS files provided separately?

Security Notices, introduced in 2014, are text (bulletin-like) documents provided on the Security Portal used to communicate information for highly publicized vulnerabilities that may generate a high degree of public or media attention. They are also used to communicate information regarding vulnerabilities for products that do not participate in the SMP/E process. In addition, Security Notices may be used to communicate new or critical information that may be needed to ensure the overall security of IBM Z in the enterprise. The Security APAR information (HOLDDATA, CVSS and ASSIGN files) are provided to evaluate the IBM Z products that provide fixes via the SMP/E process.

Security Notices will be in the format SN-YYYY-NN, where YYYY is the year of the vulnerability and NN represents the sequential number of the Security Notice. There are times when related Security Notices are grouped under the same sequential number and differentiated by a point number, such as SN-YYYY-NN.1, SN-YYYY-NN.2, etc.

If my question is not addressed in this FAQ how can I get an answer?

You can send an email to syszsec@us.ibm if you have questions about the IBM Z Security Portal. To ensue your question is routed to the appropriate team, make sure you have "Z Security Portal" in the Subject field

There is a team of people that need this information, can we register a group or service ID?

Individuals must register the Security Portal, since the individual and their management are agreeing to the terms and conditions. If the sensitive portal data went to a distribution list there is a possibility to add someone to that list that is not aware of the sensitivity or the terms and conditions. It would also undermine the yearly re-validation process.

I am not using the vulnerable function; do I still need to install the fix?

Yes, if the vulnerable function is installed on the system it needs to be updated with the latest service. A hacker or malicious user can exploit any vulnerable code that is installed on a system, not just the code you are using. It is critical to keep any code that is installed on a system up to date whether that function

is used or not by current processes, attacks can take on many forms and employ unused and unpatched code as an entry point, pass through or launch pad for a multi-step attack.

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.
Produced in the United States of America,
07/2018

ZSQ03054-USEN-05