IBM Z
and LinuxONE

April 2022

IBM Z and LinuxONE Security Portal

Frequently Asked Questions

Worldwide

ZSQ03054-USEN-06

General Questions

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

The current IBM Z and LinuxONE Security Portal (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 anda 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.

What is provided on the Security Portal?

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

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 to IBM Z clients without publicly posting information that could puttheir systems in danger. Those IBM clients decide who within their organization has a need to access the security portal, need to know.

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

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 fulldisclosure 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 provided APAR information?

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 cases, 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 iscritical that both APAR information and Security Notices are both monitored regularly in accordance with your security policy.

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/OSand 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 relevantAPAR 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.

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, inevery 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 excludemalicious 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 continueto help to mitigate enterprise vulnerability to attacks.

When there is a security concern should I expect a Red Alert or a HIPER APAR?

There is often confusion on Red Alerts and HIPERs vs. the Security Portal. The Security Portal and process has been around since the early 2000's. Likewise Red Alerts and HIPERs have been around longer. The Portal, HIPERs and Red Alerts are all part of how IBM communicates. Opposite to the Security Portal, HIPERs and Red Alerts are public, available to anyone and do not contain or communicate security or system integrity issues. Where there is sometimes confusion is that Data Integrity issues, not system integrity, are broadcast very publicly via Red Alerts and HIPER. If there is some possibility that an IBM product can cause a customer's data to be corrupted, we very quickly and loudly broadcast what they need to do to mitigate the Data Integrity concern.

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

The support 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 securityor integrity vulnerability the resulting APAR/PTF will be treated as IBM Confidential and subsequently available via the IBM Z Security Portal. For cases opened for information about security or integrity APARs/PTFs, customers will be directed to the Security Portal.

Why can't IBM support answer questions about security vulnerabilities, even when I tell them I have access to the Security Portal?

The Security Portal is the single source for security information provided to all registered customers. Each customer decides who in their company should have access to the information provided as this information can put their enterprise at risk. These individuals go through a vetting process and access controls are put in place to permit their sensitive information after agreeing to Terms and Conditions. The support team can not verify who they are talking to or the status of their access to the Security Portal. That list is kept confidential and changes dynamically.

Registration & Access

Who needs access to the Security Portal?

IBM strongly recommends that every IBM Z client register and subscribe to the Security Portal. A best practice would be to register more than one person. ensuring coverage for various out of office scenarios, such as, vacations, shifts, etc. It is also important to ensure coverage across roles, including security officer, auditor, system programmer, etc. 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 do I gain access to the Security Portal?

The instructions for access to the Security Portal can be found at https://ibm.biz/security-portal-registration

What can I expect once I submit a request for registration to the Security Portal?

Once you fill out the registration form on the web site (https://ibm.biz/security-portal-registration), entering all the required information, the IBM team will begin the vetting process. They will reach out to your IBM or Business Partner representative for their assistance. The team will verify that your company has an IBM Z or LinuxONE machine and associated operating system license. The IBM or Business Partner rep will then reach out to management at the requesting company to ensure the understanding and agreement to the Terms and Conditions. Once the agreement is in place and the required data, such as your IBMid, is provided the registration is approved and once the automation completes a note with instructions is sent to the requestor.

My registration email was misplaced, and I can't find the Security Portal?

The link for Portal Registration is often confused with the link to the actual security Portal which is hosted on ResourceLink. If the customer successfully registers for access to the Security Portal, they would have gotten an email with the link (https://ibm.biz/ibm-z-security-portal) and instructions. Select "Problem Solving" then "Security Alerts" to navigate to the Security Portal. If you follow this link and have not registered for access, you will not see the IBM Z security data.

What is the difference between being authorized and subscribed to the 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.

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.

From the "Security Alerts" page you can click "Subscribe to this page" to receive a non-confidential email when there is anything new or updated in the Security Portal. Clicking the link will subscribe you to "z Systems – Security Alerts" and take you to a page where you can manage your other subscriptions or subscribe to alerts for specific products in Resource Link as well.

Can zPDT or other emulator users register for access to the Security Portal?

No, the Security Portal is for IBM clients that have a licensed IBM Z or LinuxONE mainframe. It is not intended for users of emulators, such as zPDT, zRD&T, etc. using the z/OS ADCD or z/VM ADCD. The ADCD environment is not intended to be serviced, it is designed to be replaced regularly, as updates are tested and provided.

I am a Business Partner can I access the Security Portal?

As a Business Partner if you own an IBM Z or LinuxONE machine and associated operating system license you would be considered a customer. If you do not own an IBM Z or LinuxONE machine you would not have a need to know. The customer with the need to know would be the owner of that machine.

I am a contractor, business partner or work for an outsourcing company managing an IBM Z or LinuxONE systems for another company. Can I access the Security Portal?

We will need the manager responsible for your contract at the company that has a licensed IBM Z or LinuxONE system to be part of the request for access. They will be a critical part of the registration process as we evaluate the contract and its coverage of the Security Portal Terms and Conditions.

I recognize that the information contained in the 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 ofperforming 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 givethem 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.

I am a manager can I get access?

Yes, a manager can gain access to the Security Portal. In this case their director or VP would be engaged to ensure the understanding and agreement to the Security Portal Terms and Conditions.

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 tothe 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.

Who in my organization has access to the Security Portal?

We are happy to work with the management team in your organization to ensure the right people have access. In addition to the yearly vetting process, a manager in your organization that approves access can send an email to IBM.Z.Security.Portal.Registration@ibm.com requesting a list of those registered for access.

If I download information from the Security Portal, can I share it with the person who applies our maintenance?

It is common practice that the list of APARs/PTFs, security related or not, is applied by a person that is not in a security related role. It is important that they are not provide the security details, such as CVSS data, and are aware of the Terms and Conditions. They should only be provided with the APAR / PTF information for the patches that need to be applied regardless of their security categorization.

Security Portal Content

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 (https://ibm.biz/zos-holddata). 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 theyknow what APARs need to be installed to keep the system up to date regarding service.

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 yoursystem. Specifically, it includes for each Security / Integrity APAR the associated 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, or other aspect that affect your enterprise or security policy.

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 FIRSTweb 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 includedafter the REASON keyword. In the COMMENT you will find the PTF number follows the FIX keyword andwhen 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 twodigits 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 basisas 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 dueto the formatting of columns use a fixed width (non-proportional) font such as "courier" for viewing.

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 Portalused to communicate information for highly publicized vulnerabilities that may generate a high degreeof 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 tocommunicate new or critical information that may be needed to ensure the overall security of IBM Z inthe 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-NNN, where YYYY is the year of the vulnerability and NNN represents the sequential number of the Security Notice. There are times when related Security Noticesare grouped under the same sequential number and differentiated by a point number, such as SN-YYYY-NNN.1, SN-YYYY-NNN.2, etc.

How do I acquire Sec/Int PTFs?

After you used the date in the Security Portal to identify PTFs that need to be installed on z/OS you need to download and install the fixes. Much of this is outlined in the "z/OS Preventive Maintenance Strategy to Maintain System Availability" whitepaper (https://ibm.biz/zos-preventative-maintenance).

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 toscoring can be found on the FIRST (Forum of Incident Response and Security Teams) web site (http://www.first.org/cvss/). Base and Temporal scores are provided. If an Environmental score is required this must be computed by the client using the provided CVSS vector, taking into considerationtheir 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. Whenthe version 3 (V3) specification was introduced by FIRST, the "CVSS:3.0", and now "CVSS:3.1" prefix was added to the Vector string to differentiate between V2, V3.0, V3.1 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)

Sample CVSS V3.1 Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L)

Are the fixes for the Security / Integrity information found in the IBM Z Security Portal includedin 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 theSecurity / 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 isto help ensure you have the data as soon as possible to make the best decisions for your enterprise.

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 therisk 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 IBM Zenvironment?

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 levelagreement (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 usingthe associated color on a few example CVSS Vectors.

CVSS Version 2Metric		Values		
		Bad	Worse	Worst
AV	Access Vector	Local	Adjacent Network	Network
AC	Access Complexity	High	Medium	Low
Au	Authentication	Multiple	Single	None
C	Confidentiality Impact	None	Partial	Complete
I	Integrity Impact	None	Partial	Complete
A	Availability Impact	None	Partial	Complete

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 networkattack. Each

vector helps in the evaluation of the applicability of a fix 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 theSecurity Portal may be version 2, 3.0 or 3.1 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 protectall APAR information to minimize risk for all IBM Z clients. The client personnel that have demonstrateda 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.

Occasionally I see multiple records in the CVSS or HOLDDATA file with identical APAR information, is this a mistake?

From time to time, you may see an APAR with identical information in the CVSS file or multiple ++HOLDs for the same APAR with the same FMID across multiple days. One possibility is when an APAR has multiple PTFs (multiple release levels) and the PTFs are not all "Closed" on the same day, there can be two PTFs for the same APAR on multiple days with identical information. Since the COR Closing is an automated process, it is possible that one PTF closes just before midnight and the other PTF closes just after, posting them minutes apart, but on separate days, or for other reasons all resolving PTFs are not "Closed" on the same day. Another possibility is that the APAR is included in the Superseding APARs section of a PTF superseding the first PTF. This could trigger and send another notification when there is another COR Closed PTF fixing the same APAR.

In either case, the information is correct, and SMP/E will correctly process the HOLDDATA.

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 unpatchedcode as an entry point, pass through or launch pad for a multi-step attack.

What happens when a Security fix is PE?

When a security or system integrity fix contains an error, it is marked PE (PTF in Error) just like any other APAR. When investigating PEs which involve security or integrity fixes, customers can use the CVSS Base score, and metrics/vector data contained in the security portal to determine if removing a SEC/INT PTF is preferrable to leaving the PE on the system until a new fix is available.

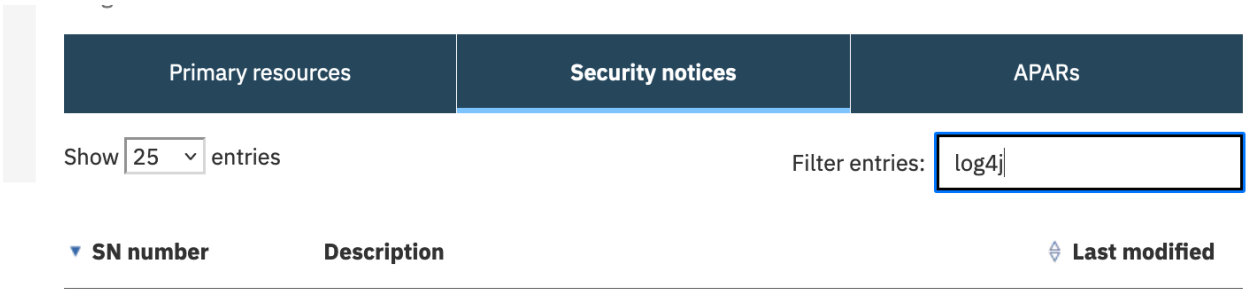
Navigating the Portal

I am having trouble locating the latest information in the 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. TheSecurity Portal has a new look and feel with the use of category tabs, enhanced search, sort and filter capabilities. The Security Portal landing page 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 we now provide 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 hasalso been refined to better highlight content within the Resource Link site.

How do I find a Security Notice?

Once signed in to ResourceLink (https://ibm.biz/ibm-z-security-portal) navigate (select "Problem Solving" then "Security Alerts") to the Security Portal (you will only see the IBM Z data if registered) you can access the Security Notices (click the "Security Notices" tab in the middle of the page). Typing "log4j" in the Filter entries box will give you the list of all the Log4j Security Notices.



It was recommended that I continue to monitor the Security Portal for updates. How often should I check?

You can choose to monitor the Security Portal on a schedule depending on your company's Security Process, however, IBM suggest that you Subscribe to the Security Portal. When you subscribe you will get an email with a link every time there is a new entry or update.

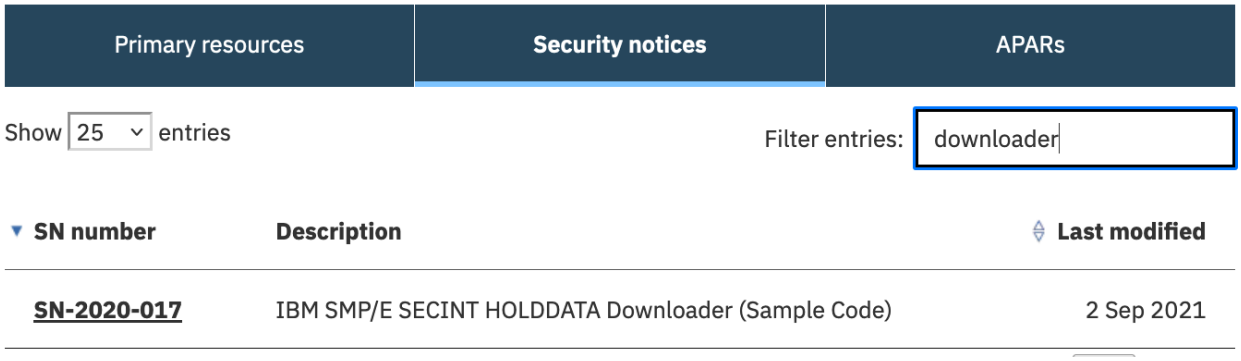
Portal Automation

Do I have to manually download files from the portal?

The integration of key files, such as HOLDDATA & ASSIGN data to support client Security Policies is critical. While some choose to do this as a manual process, others have asked for an automated integration directly to their IBM Z environment. We have provided a sample Python script, called the “IBM SMP/E SECINT HOLDDATA Downloader (Sample Code)”, to aid in automating the integrating of the security portal. The sample script is found in the Security Portal.

Where can I find the sample automation code?

In the following screen shot you can see how selecting the “Security notices” tab in the middle of the screen and using the “Filter entries” option to enter “downloader” brings you right to the Security Notice (SN-2020-017) with the sample code and instructions.



There is also a quick link to this Security Notice under the “Primary resources” tab as seen below:

Global Threat Communication

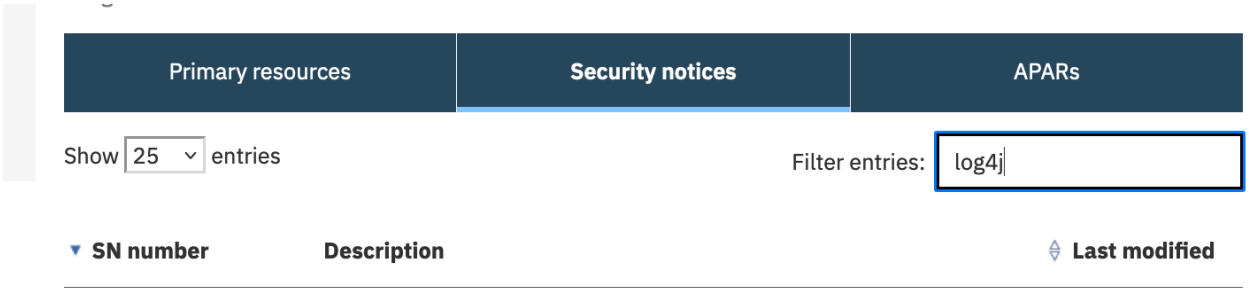
What can I expect when there is a Global Threat?

When IBM Z addresses a Global Threat a Security Notice will be created with the format SN-YYYY-nnn, where YYYY is the current year and nnn is the next number. We will then have a sub-notice noting all the products under investigation with format of SN-YYYY-nnn.0 (dot zero), the Under Investigation list. Once investigation is complete the product will be removed from the Under Investigation list and a sub-notice will be created for every product that requires a fix or mitigation with the format of SN-YYYY-nnn.x, where x will be sequential starting with 1. If the Product is not on the under-investigation list and there is no Security Notice there is not a concern for the product.

Every update to these security notices will generate an email to the customer with a link to the update, if they have subscribed to notifications.

How can I find information for a Global Threat?

The Security Portal provides a Filter function which permits the quick access to a set of Security Notices, for example entering "Log4j" in the filter box provides the complete list of IBM Z relevant Security Notices (hardware, firmware, operating system, software, etc.) in one spot.



Some products state they are NOT affected or companies provide lists of their NOT affected products. Why does IBM Z utilize Under Investigation list scheme?

Public Unaffected lists used industry wide caused a lot of confusion as products were added and removed over time. Something was added, then a customer saw they were not affected and walked away, but days later more was learned about the vulnerability and the product was taken off the list, but the customer did not know to look again. For IBM Z we used an under-investigation list and Security Notice process. If there was no Security Notice and the product was not on the under-investigation list, there was no concern. The list of vulnerable products was small compared to unaffected, so it was also easier to view the small list of products.

Why is there no "Not Applicable" list for CVEs during a Global Threat?

In the IBM Z and LinuxONE Security Portal when there is a Global threat there will be a Security Notice (SN-YYYY-xxx.0) for products under investigation and then there will be a Security Notice if there is a fix needed. If the product is not in the Under Investigation List and there is no Security Notice, then there is no concern for the stated global threat. When you consider there are over 1000 products / versions that run on IBM Z and LinuxONE the matrix of Not Applicable entries would be huge compared to the small number of products identified with Security Notices. The provided Filter function quickly highlights the area where fixes need to be applied, removing any distraction from the critical information that needs to be shared.

Communications

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

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

When do I open a Case with service?

If you have applied all the service and followed the guidance from the Security Portal for the product in question and you have a scan report, penetration test, etc. identifying a security vulnerability in an IBM Z or LinuxONE product you should follow the normal support process, sharing the details from the scan, Pen Test etc. so the security concern can be investigated and a fix provided if needed or we can identify it as false positive.

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.
04/22

ZSQ03054-USEN-06