GCOS8: Information about the Meltdown and Spectrum security* vulnerabilities:

GCOS8 systems are running Itanium CPU. Intel has reported that Itanium CPUs are not affected by these vulnerabilities. Using Intel's SA-00075 Detection and Mitigation tool Checking, shows that the SP (Service Processor) and iCare PC related to GCOS8 systems are not vulnerable. Consequently, there are no actions to perform on the GCOS8 mainframe itself and on the SP and iCare PC.

For DBSP and Virtuo systems refer below statements and apply the suitable recommendations.

Basic Workarounds and Mitigations
The most immediate action you can take to protect yourselves is to prevent execution of unauthorized software on any system that handles sensitive data.

1. Fix to apply for DBSP systems

The vulnerability concerned DBSP models with R720, R730 (DELL) and NOVASCALE R460 F3 (BULL).
To solve this vulnerability the following fix must be applied:

- For the hardware DBSP R720 and R730 (DELL) there is a new BIOS available from DELL site: http://support.dell.com
- For hardware DBSP NOVASCALE R460 F3 (BULL) use the new BIOS R720 DELL also available from DELL site http://support.dell.com
- For DBSP REDHAT software apply the software update available from RedHat site: https://access.redhat.com/security/vulnerabilities/speculativeexecution

  This put the system at the latest Red Hat 6 update available (RHEL 6.9) validated.

2. Fix to apply for Virtuo systems

There are fix to apply for the Firmware and for the Operating System:
Firmware updates for Power7+ and Power8 are available in order to mitigate CVE-2017-5715 (Spectre variant):
http://www-01.ibm.com/support/docview.wss?uid=isg3T1026811

You can download these updates from the Atos support site:
http://support.bull.com/ols/product/platforms/escala/

CVE-2017-5753 (Spectre) and CVE-2017-5754 (Meltdown) will require, as well as the firmware updates, additional AIX updates. Roll out for the AIX updates will start January 26th through Feb 12th:
https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/

***The details of the technical description can be found at:**

https://googleprojectzero.blogspot.fr/2018/01/reading-privileged-memory-with-side.html

If you have any questions or require further information, please contact your local Atos / Bull sales or customer service representative.

----------End of the document----------

GCOS8 : Information concernant les failles de sécurité Meltdown et Spectre* :

Les systèmes GCOS8 s'exécutent sur des processeurs Itanium. Intel a rapporté que les processeurs Itanium ne sont pas affectés par ces vulnérabilités. En utilisant l'outil de détection des vulnérabilités SA-00075 d'Intel, il s'avère que le SP (processeur de service) et iCare PC liés aux systèmes GCOS8 ne sont pas vulnérables. Par conséquent, il n'y a aucune action à effectuer sur l'ordinateur central GCOS8 lui-même et sur le PC SP et iCare.

Pour les systèmes DBSP et Virtuo, reportez-vous aux instructions ci-dessous et appliquez les recommandations appropriées

Solutions de base de contournement et atténuations :

La mesure la plus immédiate que vous pouvez prendre pour vous protéger est d'empêcher l'exécution de logiciels non autorisés sur tout système traitant des données sensibles.

1. Correctifs à appliquer pour les systèmes DBSP

La vulnérabilité concerne les modèles DBSP avec R720, R730 (DELL) et NOVASCALE R460 F3 (BULL).
Pour résoudre cette vulnérabilité, le correctif suivant doit être appliqué:

- Pour les matériels DBSP R720 et R730 (DELL), un nouveau BIOS est disponible sur le site DELL: http://support.dell.com
- Pour le matériel DBSP NOVASCALE R460 F3 (BULL), utilisez le nouveau BIOS R720 DELL également disponible sur le site DELL: http://support.dell.com
- Pour le logiciel DBSP REDHAT, appliquez la mise à jour logicielle disponible sur le site RedHat: https://access.redhat.com/security/vulnerabilities/speculativeexecution

Cela met le système à la dernière mise à jour de Red Hat 6 disponible (RHEL 6.9) validée.

2. Correctif s à appliquer pour les systèmes Virtuo

Il y a des correctifs à appliquer pour le firmware et pour le système d'exploitation:
Les mises à jour du micrologiciel pour Power7 + et Power8 sont disponibles afin de corriger l'impact de CVE-2017-5715 (Spectre variante):
http://www-01.ibm.com/support/docview.wss?uid=isg3T1026811

Vous pouvez télécharger ces mises à jour depuis le site de support Atos:
http://support.bull.com/ols/product/platforms/escala/

CVE-2017-5753 (Spectre) et CVE-2017-5754 (Meltdown) nécessiteront, outre les mises à jour du micrologiciel, des mises à jour AIX supplémentaires. Le déploiement des mises à jour AIX commencera le 26 janvier et se terminera le 12 février:
https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/

*Le détail de la description technique se trouve à l'adresse :

https://googleprojectzero.blogspot.fr/2018/01/reading-privileged-memory-with-side.html

Si vous avez des questions ou souhaitez obtenir des informations complémentaires, veuillez contacter votre représentant local des ventes ou du service clientèle Atos / Bull.

----------Fin du document----------