QualityNet | AWS Cloud

January 13, 2022

Notification regarding MS Windows patch causing possible issues

BLUF – Microsoft released a vulnerability patch that can cause a bootloop condition on the patched instances. HIDS will be in direct contact for the ADOs that have applied this defective patch. **While there were a few HCQIS ADOs that applied these defective patches before they were unpublished by Microsoft, the good news is based on the Microsoft user community feedback HIDS does not expect to realize any adverse impact on HCQIS Cloud Windows instances running these patches.**

****

Details:

- Microsoft released patches during the 1/11/2022 patch Tuesday release schedule.

- On 1/12/2022, there were multiple reports from the Microsoft user community that the patch was causing a bootloop condition on various systems including Domain Controllers and Hypervisors running Microsoft Hyper-V.

  Reference articles:

  – Bleepingcomputer.com
  – Malwarebytes.com

- After receiving this community feedback, Microsoft has unpublished the defective patches, KB5009624 (for Windows 2012R2) and KB5009546 (for Windows 2016), via Windows Update.

  – Please note that there has been no official notification/update regarding this from Microsoft at this time.

- **While there were a few HCQIS ADOs who applied these defective patches before they were unpublished by Microsoft, the good news is that, based on the Microsoft user community feedback, HIDS does not expect to realize any adverse impact on HCQIS Cloud Windows instances running these patches.**

- Until Microsoft publishes updated patches, the HCQIS Community will see that the Tenable scanner has flagged any Windows instance that does not have the defective patch installed as requiring it. The following are the critical finding's plugin IDs:

  Plugin ID: 156619 - "Windows 2016"

  Plugin ID: 156624 - "Windows 2012r2"

  – HIDS has made the ISG ISSOs and HIDS Security aware of the expected critical findings and that currently there is no remediation plan until Microsoft publishes updated patches.

- The HIDS Cloud team is monitoring the situation and will provide information/updates as the scenario progresses.

****

Next steps if you applied the defective patches: Manually uninstall the patch.

KB5009624 for 2012
KB5009546 for 2016

Next steps if you are experiencing the bootloop condition: Restore the instance from a previous snapshot.

****

Note: This is an auto-generated message. Please do not respond directly to this email. If you need assistance, email dl-HCQIS-Cloud-Leads@ventechsolutions.com

---

If you need additional information, please contact us by phone at 1-866-288-8914, Slack at #help-service-center-sos, or by email at ServiceCenterSOS@cms.hhs.gov