Dear Registry Operator,

Recently, there were three issues with the Centralized Zone Data Service (CZDS), all of which have subsequently been resolved.

Towards the end of March, ICANN org was notified by a CZDS user of an issue in the system that allowed users with expired approvals to access zone files. After switching to daylight saving time, the misconfiguration prevented access rights from expiring. The issue was resolved by manually expiring these requests, and restarting the necessary services at ICANN org servers.

Subsequently, ICANN org was notified by a community member that a zone file that was downloaded from CZDS was incomplete. After learning of the error, ICANN org conducted an investigation and applied a fix to address the issue. However, the fix caused IP addresses and port numbers of the hidden servers (used by registry operators to share zone files with ICANN org) to become visible to those CZDS end-users that may have accessed zone files between 8-11 May 2020. The zone files that included the IP addresses and port numbers were removed from CZDS on 11 May 2020, and precautions were put in place to prevent reoccurrence.

In keeping with ICANN's commitment to transparency, this information has also been published on our cybersecurity incident log. We thank the individuals for reporting these issues and encourage others to report potential concerns to ICANN org by emailing vulnerability@icann.org.

Regards,

Russ Weinstein

Senior Director, gTLD Accounts and Services ICANN