Dear Contracted Party,

As you may be aware, a widespread vulnerability with a Java-language software utility for Apache servers was reported for global visibility by a security researcher on Friday, 10 December. This is not a directed attack on ICANN. The Apache server is a widely used, free, and open-source solution that delivers web content through the Internet. This particular vulnerability, technically referred to as CVE-2021-44228, allows an attacker to send an authorized request to various websites or devices that could allow the attacker to access, change or delete various services. This vulnerability has impacted millions of web resources across the Internet.

All ICANN-managed websites and publicly facing systems have been assessed, and a patch provided by the Apache Foundation has been applied to ICANN's various systems to prevent exploitation. We are aware of the second patch and are taking appropriate action. There is no indication that any ICANN website or system has been accessed by any unauthorized users. ICANN is continuing to run additional tests on all ICANN managed systems. This includes off-the-shelf solutions that may require a patch from the respective vendors to guard against exploitation. When patches are made available by these third-party providers they will be applied. Please be aware this may result in temporarily taking a website or service offline for maintenance. Should this occur, thank you in advance for your patience.

If you haven't already done so, we urge you to assess your systems as well.

Sincerely,
Russ Weinstein
Vice President GDD Accounts and Services