External Incident Report – Draft

Date: March 29, 2024

Title: govAccess – Vision – Sites Unavailable on Internal Networks	**Current Status:** Resolved
Incident Start Date/Time: March 25, 2024, 10:32 AM CT	**Incident End Date/Time:** March 26, 2024, 5:56 PM CT

Executive Summary (All times in CT (Central Time))

At 10:32 AM on Monday, March 25, 2024, Granicus Customer Support notified Engineering Teams of customers reporting Vision websites were inaccessible. The Incident Response Team opened a bridge to investigate and restore services.

Investigations revealed that this issue was intermittent and affecting a subset of customers. The cause of the issue was traced back to a routine DNS (Domain Name System) migration performed over the weekend that required DNS records to propagate.

At 11:15 AM, a workaround was identified and relayed to customers via support tickets. The workaround asked customers to temporarily reconfigure their DNS forwarder to point to a public DNS while Engineers continued to troubleshoot the core issue.

Around 3:53 PM, a small subset of affected customers began to report receiving CloudFlare 1016 errors while attempting to access their sites from internal networks. Customers affected by this error were contacted via Customer Support and asked to either disable or refresh their CloudFlare DNS proxy. This resolved the 1016 error.

The following morning, Customer Support relayed to the Engineering Teams that customers were reporting the temporary workaround to reconfigure their DNS forwarder and point to a public DNS was no longer working. At 12:20 PM CT, the teams determined that DNSSEC was required but not enabled on the new DNS account. By 12:37 PM, the teams had re-enabled DNSSEC which solved root cause. However, due to internet DNS propagation times, a full recovery for all customers was estimated to take up to 24 hours. Monitoring continued throughout the day, and the issue was declared resolved at 5:56 PM upon reception of positive feedback from multiple customers.

Action to Resolve

DNSSEC was enabled on the DNS domain account. The smaller subset of customers who received 1016

errors were further solved by them disabling or refreshing their CloudFlare DNS proxies.

Root Cause

A routine DNS server migration implemented on the night of Friday, March 22 did not enable DNSSEC on the new account which caused validation failures for some customers. DNSSEC was re-enabled and, once propagated to the customers' respective DNS, resolved the issue.

Impact

Some Vision customers were unable to access their websites from internal networks until DNS propagation was completed.

After Action Steps

- Advise customers via support tickets to have their external DNS forwarder providers flush their caches and verify that they can resolve granicusgovaccess.net if they are still experiencing issues. - **In Progress**
- Internal communications and processes, including routine migration, are being reassessed and adjusted. - **In Progress**
- Instituting DNS test domains to mimic customer internal environments to improve troubleshooting are being investigated. - **In Progress**