TechBrief

Liquidware Remediation Plan Response with 6.6.2-6

Apache HTTPD

Fix the subject's Common Name (CN) field in the certificate.

This finding is due to default configuration of a self-signed certificate on the appliance. Liquidware would suggest placing signed SSL certificates on the appliance to remediate the issue. Here is the link to document with instructions: Placing Signed SSL certificates on the Appliance.

Disable any weak HMAC algorithms within the TLS configuration.

Stratusphere UX 6.6.2-6 addresses this finding by applying the recommended cipher configuration as part of the patch installation:

```
ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSACHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-ECDSA-AES256- SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-
SHA256:ECDHE-RSA-AES128- SHA256:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK:!SHA1:!DSS
```

Disable TLS/SSL support for static key cipher suites.

Stratusphere UX Web Server uses the Intermediate Configuration. It accepts TLS 1.2 and higher, that includes 1.3. Access to the Web UI through browsers configured to use only TLS 1.3 works in the current version. However, due to the requirement of being backward compatible for accepting data from older versions of CID Key agents does NOT allow us to move to Modern Configuration that only supports TLS 1.3.

Generate random Diffie-Hellman parameters.

Liquidware follows Department of Defense and Federal security guidelines to meet security requirements. Using random Diffie-Hellman parameters affects FIPS compliance which is a requirement in high security environments. Liquidware follows the recommendations from Red Hat 8 Security Hardening guidelines for Diffie-Hellman parameters which also maintain FIPS compliance. The recommendations are available at Red Hat 8 Security Hardening: Using the System Wide Cryptographic Policies.

We have also made changes in Stratusphere 6.6.2-6 suggested by the original researchers WeakDH.org as part of the remediation steps. However, due to FIPS compliance requirements, we could NOT implement "`openssl dhparam -out dhparams.pem 2048`" because it breaks our FIPS requirements for our federal customers.

For Postgres

Restricting database access.

Liquidware provides an Enhanced Security Configuration for highly secure networks such as those within the Department of Defense. Liquidware would recommend this configuration for stronger security posture. Here are instructions: Stratusphere Security Configuration Addendum.

Alternatively, if Enhanced Security Configuration is too involved, Liquidware could provide instructions to manually restrict access to the database to trusted systems on your specific installation. However, this approach may NOT stick after an upgrade. For a more permanent change, Liquidware will need to make code changes to alter the current behavior and configuration of the Firewall onboard the appliance. These changes will take more time to develop & certify through our QA process. We plan to make this available as part of our next version 6.7.5 scheduled for Q3 2024.

For OpenBSD OpenSSH 8.0

Disable any MD5 or 96-bit HMAC algorithms within the SSH configuration.
Liquidware software is FIPS compliant where it must use a minimum of 256-bit or higher keys. The default OpenSSL configuration onboard the appliance does include other settings, but they are not used due to FIPS requirements. We override the defaults OpenSSH configuration with those defined in `/usr/share/crypto-policies/FIPS/opensshserver.txt`, specifically the HMAC configuration: hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha1,hmac-sha2-512.

CVEs Included in Stratusphere UX 6.6.2-6

Here is a list of CVEs included:CVE-2020-22217, CVE-2022-3094, CVE-2022-44638, CVE-2022-45884, CVE-2022-45886, CVE-2022-45919, CVE-2022-48337, CVE-2022-48339, CVE-2023-1192, CVE-2023-2162, CVE-2023-2163, CVE-2023-3138, CVE-2023-3341, CVE-2023-3812, CVE-2023-4863, CVE-2023-5178, CVE-2023-5981, CVE-2023-7104, CVE-2023-28484, CVE-2023-29469, CVE-2023-31130, CVE-2023-31486, CVE-2023-33204, CVE-2023-33285, CVE-2023-34410, CVE-2023-37369, CVE-2023-38197, CVE-2023-39615, CVE-2024-0985, CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-20926, CVE-2024-20945, CVE-2024-20952, CVE-2023-4622, & CVE-2023-42753.