Presented By
Shera Mui
Network Applications Supervisor

SECURITY ENHANCEMENT FOR MAINFRAME SERVICES

Why Secure Your Connections?

Our goal is to eliminate potential threat and reduce the vulnerability from open clear-text sessions being sniffed for credentials and information on servers, mainframe, WAN, LAN, and Internet. This policy is being mandated across all server platforms.

- Communications that are sent in clear text can include usernames and passwords along.
- Data being viewed or transmitted could potentially contain sensitive data like social security numbers and health records.
- Federal and control agency audits: Audit reports identify and red flag clear-text transmissions in violation of Federal and State policies.
  - PCI (Payment Card Industry)
  - FTI (Federal Tax Information)
  - HIPPA (Health Insurance Portability and Accountability Act)

Security Enhancements

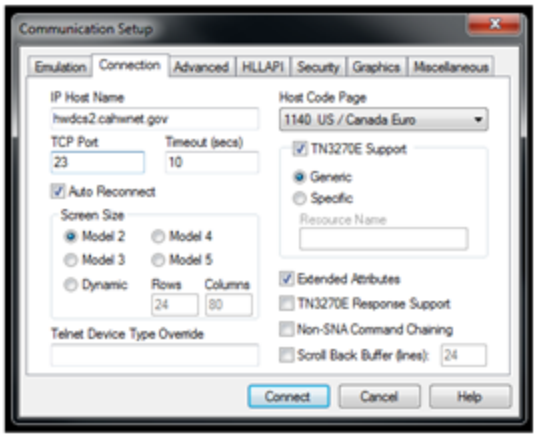
- Transport Layer Security (TLS) has been enabled for FTP (FTPS) and Telnet (TN3270) on the standard protocol ports of 21 and 23.
- No need to submit a firewall request, if you have access to these ports today you will have access to the TLS version.
- Change your sessions parameters to use TLS now, no need to delay or wait until the deadline.
- SSLv3 (Secure Socket Layer) has been disabled on port 21 and 23 to remediate the risk of the POODLE vulnerability, a man-in-the-middle exploit.
- Port 2121 (Current FTPS SSL/TLS-only) and port 2323 (SSL/TLS-only) will continue to be supported. SSLv3 support will be removed by January 2016.

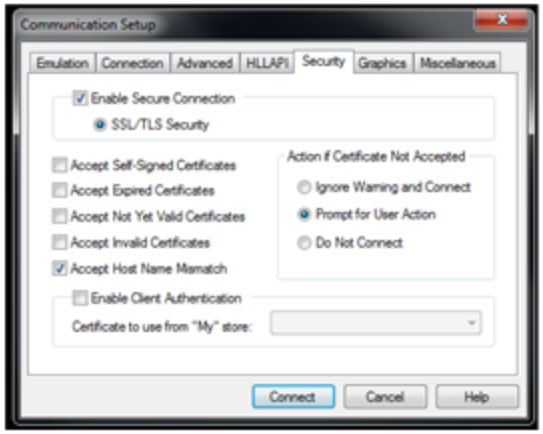
Does this effect me?

- If you see this screen when accessing mainframe applications you are likely to be effected. These are the OTech mainframe TN3270 welcome screens.

- Any FTP transmissions to the mainframe FTP Server. Check you FTP desktop clients and batch jobs, do they target an OTech mainframe using port 21 in the software settings or job?

Example: Tn3270 emulator settings

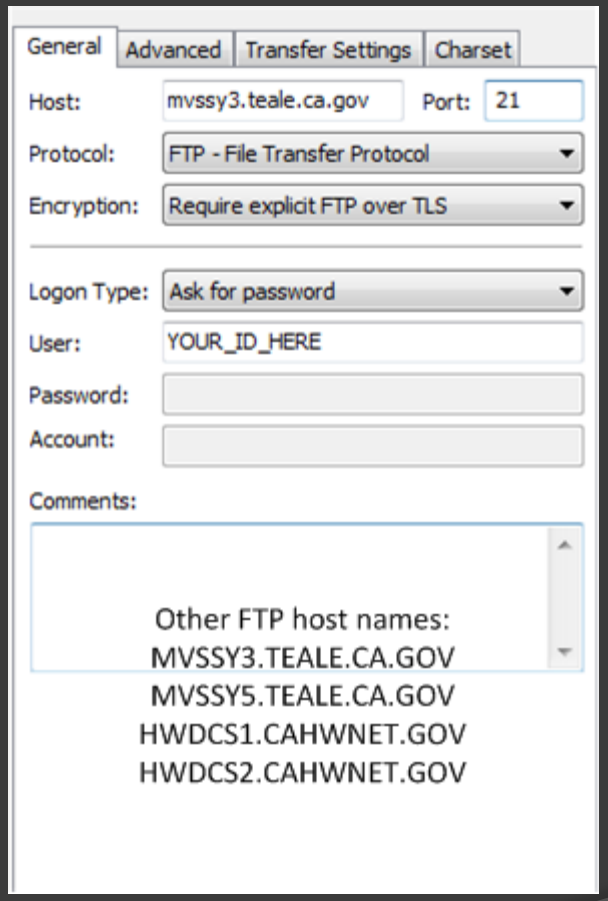




HOSTNAME may be one of the following:
HWDC3270.CAHWNET.GOV
HWDCS2.CAHWNET.GOV
DTS3270.DTS.CA.GOV
MVSSY5.TEALE.CA.GOV
MVS.TEALE.CA.GOV

**Hostname mismatch may need to be allowed, security certificate authorities only allow one hostname or DNS to be defined to the certificate. Our mainframes often have several DNS names associated to the same host.

Example: FTPS settings



Tentative Target Dates when clear-text sessions will be disabled

- **Telnet/TN3270 Target Dates:**
- Stage 1: SY9, SY0, Test, TST2 (08/05/2015 - 08/14/2015)
- Stage 2: SY8 (08/17/2015)
- Stage 3: SY3 (08/23/2015)
- Stage 4: SY2, SY4, SY6, SY7 (09/06/2015)
- Stage 5: SCT1, SCT2 (09/12/2015)
- Stage 6: SOC (09/17/2015)
- Stage 7: SOCP (09/27/15)
- Stage 8: SY5 (10/04/15)
- Stage 9: S1S1 (10/12/2015)
- Stage 10: S2S2 (11/09/2015)

- **FTP Target Dates:**
- Stage 1: SY9, SY0, Test, TST2 (08/05/2015 - 08/14/2015)
- Stage 2: SY8 (08/24/2015)
- Stage 3: SY3 (09/13/2015
- Stage 4: SY2, SY4, SY6, SY7 (09/20/15)
- Stage 5: SCT1, SCT2 (10/10/2015)
- Stage 6: SOC (10/15/2015)
- Stage 7: SOCP (10/25/2015)
- Stage 8: S1S1 (10/26/2015)
- Stage 9: SY5 (11/01/2015)
- Stage 10: S2S2 (11/23/2015)

Contact Information

If you have questions or need further clarification regarding the project please contact your CalTech Account Lead. If you are unsure who your Account Lead is, call the Customer Delivery Division at (916) 431-5476.

If you are trying to configure a TLS session and are having difficulties contact the OTech Service Desk (Service.Desk@state.ca.gov or (916) 464-4311) and open a work order for assistance.