**Securing NIM with SSL Mode: Strengthening Command Syntax Validation and Execution Restrictions**

This iFix delivers a robust security framework for NIM by enhancing **mutual certificate-based authentication**, **strict command validation**, and **secure key management**.

**Key Enhancements**

**Mutual Certificate-Based Authentication**

* Replaces traditional hostname-based trust with robust mutual TLS authentication.
* Both the client and server are required to present valid certificates and verify each other’s identities, ensuring secure and authenticated communication.
* TLS-based authentication is complemented by certificate validation, hostname verification, and IP address checks.

**Command Execution Hardening**

* The master (server) now enforces strict validation of incoming requests, allowing only predefined allowlist of NIM commands.

**Secure Key and Certificate Management**

* Eliminates insecure key distribution methods such as TFTP.
* Ensures certificates and keys are stored in a protected location, accessible only to authorized users

**NIM iFix Installation Guidelines**

* **No Additional Configuration for SSL-Enabled Setups**
* If your NIM environment already uses SSL/TLS for communication between the server (formerly master) and clients, no further configuration is needed.
* The iFix installation seamlessly integrates with your existing SSL/TLS setup.
* **Installation Order: Install Clients First, Then Server (Master)**

Two separate iFix packages are provided: one for NIM clients and one for the NIM server (master). Follow the steps in this sequence:

* Install the client iFix on all NIM clients.
* After all clients are completed, install the server iFix on the NIM server (master).
* For NIM High Availability environments, apply the server (master) iFix to both the server (master) and the alternate server (master). Once the server (master) iFix is installed, run niminit from both the server (master) and the alternate server (master) using the CLI.

⚠️ Installing the iFix on the server (master) system before applying it to the client may disrupt the existing communication between server (master) and clients. To prevent any sort of communication issues, please ensure the client iFix is installed on the clients before the installing server (master) iFix on server (master).

* **Consistent Installation Across the Environment**
* The iFix must be applied uniformly, either to the NIM server (master) and all its clients, or to none.
* If the server (master) is configured with SSL, all clients must also run in SSL mode.
* **SPOT Resource Requirements**  
  If you're using SPOT for network boot or OS installation, ensure the client-side iFix is applied to the corresponding SPOT resource to maintain consistency and functionality.

**Note:** When installing the iFix on the SPOT, export the following variable:

export FORCE\_SCRIPTS=yes

* **Includes Prior Vulnerability Fixes**

# This iFix includes the NIM vulnerability iFix that was delivered in the March [CVE-2024-56346, CVE-2024-56347](https://www.ibm.com/support/pages/security-bulletin-aix-vulnerable-arbitrary-command-execution-cve-2024-56346-cve-2024-56347)

* **Enabling SSL in Non-SSL Environments**   
  Addressing the vulnerability requires configuring NIM in SSL/TLS Secure mode (nimconfig -c) and applying the fixes provided in this bulletin.

→ Refer to: [Preparing to enable cryptographic authentication](https://www.ibm.com/docs/en/aix/7.3.0?topic=authentication-preparing-enable-cryptographic) and

[Enabling cryptographic authentication from the command line](https://www.ibm.com/docs/en/aix/7.3.0?topic=communication-enabling-cryptographic-authentication) for detailed steps

* **Creating additional interface attributes:**  
  In environments where NIM is configured with SSL (nimsh secure mode), the SSL certificates on the NIM server (master) must be refreshed after adding or removing network interfaces. This ensures that the certificates accurately reflect the updated interface configuration and maintain secure communication.

For more details, refer to the IBM documentation: Creating additional interface attributes:

<https://www.ibm.com/docs/en/aix/7.3.0?topic=nim-creating-additional-interface-attributes>