ADV-2025-03-17 - VPN Client Privilege Escalation

1. Overview

The IXON VPN client is vulnerable to a Local Privilege Escalation (LPE) to root/SYSTEM by executing a configuration file which can be controlled by a non-privileged user.

2. Affected products and versions

- **Product name**: IXON VPN Client (Windows, Linux & macOS)
- **Affected versions**: v1.4.3 and lower

3. Patched versions

- **Patched versions**: v1.4.4 and later (addresses CVE-2025-26168 and CVE-2025-26169)

4. Impact of vulnerability

The vulnerability allows a local non-root attacker to escalate to root or SYSTEM privileges on systems with the IXON VPN Client installed. This occurs through a race condition exploit, where an attacker can overwrite the temporary OpenVPN configuration file located in a world-writable directory. By injecting malicious commands into the configuration file prior to its execution by the VPN client, an attacker can trigger arbitrary code execution with root/system privileges when a VPN connection is initiated.

5. Instructions to apply the patch

See this Support Article for instructions to install the patch. Alternatively:

1. **Download**: Obtain the updated software from https://portal.ixon.cloud/fleet-manager/tools
2. **Installation**:
   - **Windows & macOS**: Run the installer.
   - **Linux**: Execute the following commands in a terminal:

```
tar -xzf vpn_client_x64.tar.gz
cd vpn_client_x64
sudo ./install
```