CERT-In Vulnerability Note CVE-2022-40630
Session fixation

Original Issue Date: September 09, 2022

Severity Rating: Medium

Software Version Affected: 19.1.1 – 22.20.1

Overview

Session Fixation Vulnerability reported in Tacitine Firewall UI in version 20.3.1

Description

A malicious user can specify their own session token value and the value of the session cookie is not changed by the server after successful authentication and the session token will also remain unchanged for the user independently of how many times they have authenticated.

Solution

Option:1

Hotfix patch packages are deployed for auto software updates on 10 Sept 2022
Hotfix patch Packages are available for manual uploaded

Patch file name:
For software version 19.1.1 – 20.3.1: p16_103_security_updates_1.tpp
For Software version 21.1.1 and above: p20_106_security_updates_3.tpp

Option:2

Upload to latest software version 22.21.2
(available in firewall Software Management page for auto update)

Incase of manual updates of the above patches contact support@tacitine.com