



CERT-In Vulnerability Note CVE-2022-40628

Remote Code Execution Vulnerability

Original Issue Date: September 09, 2022

**Severity Rating:** CRITICAL

Software Version Affected: 19.1.1 – 22.20.1

### **Overview**

Unauthenticated Remote Code Execution Vulnerability reported in Tacitine Firewall UI in version 20.3.1

### **Description**

A remote code execution vulnerability exists in the Tacitine firewall products. An unauthenticated, remote attacker can exploit this and execute arbitrary commands via management interface

### **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](mailto:support@tacitine.com)