PRIXL

PRIXL FACT SHEET

Attacks on CA Firm Servers, 2026

Six months of Prixl Warden data, on one page

October 2026 · Prixl Technologies

3.9 million
password attempts from the internet against three CA firm servers, March to October 2026

143,259
attempts on one server in a single day, almost two a second

1 min 52 s
from switching on monitoring of a new cloud server to its first password attack

142
countries the attacks came from, India the largest at 25.7%

61.8%
of attempts tried the username "administrator"

1 in 5
attacking addresses tried more than one firm

65.5%
of attempts arrived outside office hours, evenly across the clock

99.97%
fewer password attempts reached the server once Remote Desktop was closed to the internet, on the server we watched

Attackers know their audience. After "administrator" and "admin", they try "accounts", "finance", "audit" and ten usernames built on "tally".

A switched-off firewall reopens what you closed. When one server's firewall went off, the first attack came about half an hour later and more than 370,000 followed in five days.

What to do. Close Remote Desktop to the internet and use a VPN. Keep all three firewall profiles on and check after installing software. Do not sign in as Administrator. Turn on account lockout, including for the built-in Administrator. Make alerts reach a phone. Prepare for CERT-In's six-hour reporting rule.

Source: Prixl Technologies, *Remote Desktop Under Attack*, October 2026. Three customer servers at three CA firms in India plus Prixl's cloud test servers; failed sign-ins from public addresses recorded by Prixl Warden. IP Geolocation by DB-IP, CC BY 4.0. Full paper and a free Information Security Policy template at prixl.io.