Check Point releases emergency hotfixes for zero-day exploited to gain root access



Check Point has issued emergency hotfixes for a high-severity flaw that attackers have exploited since late October to obtain root privileges and maintain persistence on vulnerable devices.

- Check Point Software has released emergency hotfixes for a high-severity zero-day flaw.
- Attackers have been exploiting the flaw since late October.
- Successful exploitation gives root privileges on vulnerable devices.
- Attackers have also used it to establish persistence on affected devices.

What happened

Check Point Software has released emergency hotfixes for a high-severity zero-day vulnerability. According to

the report, attackers have been exploiting it since late October to gain root privileges and establish persistence on vulnerable devices.

The source excerpt does not name the affected products or versions, and it gives no CVE identifier. Those details should be taken from Check Point's own advisory.

Why it matters

Root access gives an attacker full control of a device. Persistence means that access may survive a reboot or routine changes. Because exploitation began in late October, a device that was exposed during that period may already be compromised, so applying the fix alone may not be enough.

Recommended approach

Security teams should confirm quickly whether any Check Point devices in their estate are in scope, apply the vendor's hotfixes, and review those devices for signs of earlier compromise. Findings and decisions should be recorded as part of normal vulnerability and incident handling.

What to do now

1. Identify all Check Point devices in your estate and check them against the vendor's advisory.
2. Apply the emergency hotfixes on affected devices as a priority, under emergency change control.
3. Review affected devices for signs of compromise dating back to late October, including unexpected accounts, processes or configuration changes.
4. Escalate any suspected compromise through your incident response process and notify the relevant authorities as your obligations require.
5. Record the exposure assessment and remediation in your vulnerability management register.