SonicWall Urges Customers to Retire Gen 6 Firewalls, Which Will No Longer Receive Security Patches



SonicWall has told customers still running Generation 6 firewalls to retire and replace them now and stop exposing them at the internet edge. The devices will get no security patches, even for critical flaws.

- SonicWall urges all customers on Generation 6 firewalls to retire and replace them immediately.
- The vendor says Gen 6 devices will not receive security patches, even for critical vulnerabilities.
- Customers are told to stop exposing these devices on the internet edge.
- SonicWall cites attackers using automation and AI to find and exploit unsupported edge devices faster.
- The source does not list specific CVEs or confirmed incidents.

SonicWall has issued a warning to customers who still operate Generation 6 firewalls: the devices should be retired and replaced immediately, and they should no longer be exposed on the internet edge.

What the vendor says

According to the report, Gen 6 firewalls will not receive security patches, including for critical flaws. SonicWall's reasoning is that attackers now use automation and AI to find and exploit unsupported edge devices faster than before, and it expects internet-facing Gen 6 firewalls to be targeted.

The source excerpt does not name specific vulnerabilities, give dates, or describe confirmed compromises, so this should be read as a vendor end-of-support warning rather than a report of a particular exploit.

Why it matters for regulated institutions

A perimeter firewall that can no longer be patched is a standing exposure. Any flaw found in future will stay open on a device that sits at the boundary between the internal network and the internet. For institutions subject to NCA and SAMA requirements, running unsupported technology at the edge is difficult to justify in risk assessments and audits.

The practical response is to establish quickly whether any Gen 6 units remain in service, including in branches, remote sites and with third-party operators, and to plan their replacement with clear priorities based on exposure.

What to do now

1. Inventory all SonicWall firewalls and identify any Generation 6 units, including at branches and managed by third parties.
2. Remove Gen 6 devices from direct internet exposure as soon as possible, or restrict access while replacement is arranged.
3. Plan and prioritise replacement, starting with units at the internet edge.
4. Record the unsupported devices in the risk register with an owner, interim controls and a target retirement date.
5. Increase monitoring of logs and access attempts on any Gen 6 firewall that must stay in service temporarily.