SonicWall patches CVSS 10.0 pre-authentication flaw in SMA1000 appliances



SonicWall released hotfixes for four flaws in SMA1000 remote-access appliances. The most serious, rated CVSS 10.0, lets an unauthenticated attacker send requests through the device to internal functions.

- SonicWall issued hotfixes for four vulnerabilities in SMA1000 appliances.
- SMA1000 devices give remote workers access to corporate networks and applications.
- The most serious flaw is rated 10.0 on the CVSS scale.
- An attacker needs no login to send requests through the appliance and reach internal functions.
- SonicWall says it has no evidence that any of the four flaws is being exploited.

SonicWall has published hotfixes for four vulnerabilities affecting its SMA1000 appliances, the gateways organisations use to give remote workers access to internal networks and applications.

What was disclosed

The most serious of the four flaws is rated 10.0 on the CVSS scale, the maximum score. According to the report, an attacker who has no login could use it to send requests through the appliance and reach internal functions. The source does not detail the other three flaws here.

SonicWall states that it has no evidence that any of the four flaws is being exploited. That is reassuring, but it is not a reason to delay: a pre-authentication flaw on an internet-facing gateway is exactly the kind of weakness attackers study once a fix is public.

What to do next

Institutions running SMA1000 should confirm which of their appliances are affected, apply the hotfixes through their normal emergency change process, and review recent appliance logs for unusual requests. Treat the work as priority remediation for externally exposed remote-access infrastructure, and record the decision and completion date for audit purposes.

What to do now

1. Identify all SMA1000 appliances in your estate and check them against SonicWall's advisory.
2. Apply the released hotfixes through an expedited change process.
3. Review appliance and perimeter logs for unusual or unexpected internal requests.
4. Restrict management interfaces and limit exposure of the appliance to what is necessary.
5. Document the remediation and completion date for ECC and SAMA CSF audit evidence.