

NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-76071

Summary

CVE-2026-76071 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. Netis NC63 firmware through V3.0.0.3327 contains a stack-based buffer overflow vulnerability that allows unauthenticated remote attackers to overwrite saved stack state by supplying an oversized destHost parameter to the ipFilterList=mod action in netis.cgi. Attackers can exploit widthless sscanf conversions that copy user-supplied input into fixed-size stack buffers before authentication is verified, achieving remote code execution as root due to the Boa web server executing the CGI environment with root privileges.

What we know

- **CVE:** CVE-2026-76071
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.8 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.