NETS CYBER INSIDER

Edition I | November 2026

Security Vulnerabilities Affecting Enterprise Technologies

This edition of NETS Cyber Insider covers 05 security vulnerabilities affecting Barracuda, Google Chrome, OpenSSH, and SonicWall technologies.

01 | Barracuda Email Security Gateway | CVE-2026-116606

CRITICAL

Vulnerability Type	Pre-Authentication Authorization Bypass (CWE-287)
Description	A pre-authentication authorization bypass vulnerability in Barracuda Email Security Gateway versions earlier than 9.4.0.030 allows an unauthenticated remote attacker with access to the appliance's administrative interface to invoke the configuration-import function and restore a crafted, compatible backup archive, resulting in unauthorized modification of the appliance's global configuration.
Affected Versions	Email Security Gateway (ESG) firmware branches 9.4.017 and earlier.
Fixed Version	Apply Barracuda security patch BNSF-40425 (9.4.017+ firmware branch) or BNSF-40430 (<9.4.017 branch); upgrade to firmware 9.4.0.030 or latest available release.
Recommended Action	Apply the designated vendor security patch immediately, verify firmware branch with Barracuda PSIRT, and restrict appliance administrative interface access from untrusted external networks.

02 | Barracuda Multiple Products – CVE-2026-111560

HIGH

Vulnerability Type	OS Command Injection (CWE-78)
Description	An OS command injection vulnerability exists in the administrative web in-terface of multiple Barracuda appliances. An authenticated administrator can inject operating system commands through specially crafted timezone configuration parameters to execute arbitrary commands with root privi-leges. While requiring administrative access, chaining this vulnerability with the pre-authentication bypass (CVE-2026-116606) enables full unauthenticated remote compromise.
Affected Versions	Email Security Gateway (ESG, up to 9.4.0.27), Load Balancer ADC (up to 6.4.0), Message Archiver (BMA, up to 5.5.4.0), WAF Control Center (WCC, up to 2.2.1), Web Application Firewall (WAF, up to 11.0.1), Web Security Gateway (WSG, up to 16.1.100.100).
Fixed Version	ESG: BNSF-40425 / BNSF-40430 | ADC: BNADC-16586 | BMA: BNMA-32468 | WCC: BNWF-60060 | WAF: BNADC-16586 | WSG: BNYF-24789.
Recommended Action	Apply product-specific security patches across all affected Barracuda appliances immediately and isolate management interfaces behind strict net-work access controls.

Book Your Cybersecurity Consultation With NETS →

03 | Google Chrome – CVE-2026-125350

HIGH

Vulnerability Type	Use-After-Free in XML (CWE-416)
Description	A use-after-free vulnerability exists in Google Chrome's XML parser component. A remote attacker can trigger memory corruption by inducing a user to access a maliciously crafted web page, potentially leading to unauthorized program behavior or memory corruption. Google reports that an exploit for this vulnerability exists in the wild (0-day exploitation).
Affected Versions	Windows/macOS: versions earlier than 157.0.8103.51; Linux: versions earlier than 157.0.8103.50.
Fixed Version	Google Chrome 157.0.8103.50/.51 for Windows and macOS; 157.0.8103.50 for Linux. (Non-Chrome Chromium based browsers require vendor-specific updates).
Recommended Action	Upgrade all Google Chrome instances across Windows, macOS, and Linux endpoints to version 157.0.8103.50/51 or later and relaunch browser sessions immediately.

04 | OpenSSH on affected Linux configurations – CVE-2026-123158

HIGH

Vulnerability Type	Authentication Bypass (SSHole)
Description	An authentication bypass vulnerability, known as SSHole, affects OpenSSH server (sshd) running on Linux systems using the musllibc library without PAM support where password authentication is accepted. A remote unauthenticated attacker can submit a specially sized password string to bypass authentication routines and gain unauthorized shell access. (MITRE CNA CVSS: 8.1 High; Red Hat CVSS: 9.8 Critical. Red Hat products are not affected.)
Affected Versions	OpenSSH versions prior to 10.6p2 running specifically on Linux with musl libc, without PAM, where password authentication is accepted.
Fixed Version	Upstream OpenSSH 10.6p2. Administrators should consult distribution specific security advisories, as affected distributions may backport fixes independently of upstream version numbers.
Recommended Action	Update OpenSSH packages via the Linux distribution package manager immediately, enable PAM if supported, or enforce SSH public key authentication and disable password authentication (Password Authentication no).

05 | SonicWall SonicOS SSLVPN – CVE-2026-19868

HIGH

Vulnerability Type	Authentication Enforcement Bypass / Use of Single-Factor Authentication (CWE-308)
Description	An authentication enforcement vulnerability in SonicOS SSLVPN allows a user with valid credentials for an alternate authentication method to bypass SAML authentication controls. Successful exploitation may also bypass SAML-enforced multi-factor authentication (MFA). This vulnerability affects SSLVPN only when SAML authentication is enabled.
Affected Versions	SonicWall SonicOS Gen 7 firmware 7.3.3-7015 and earlier; Gen 8 firmware 8.2.2-8015 and earlier (when SAML is enabled for SSLVPN).
Fixed Version	Gen 7: Upgrade to SonicOS 7.3.4-7013 or later. Gen 8: Upgrade to SonicOS 8.2.3-8015 or later.
Recommended Action	Upgrade SonicWall Gen 7 and Gen 8 appliances to designated fixed firmware releases immediately, verify MFA/SAML configuration on SSLVPN endpoints, and audit active VPN sessions

Register Now to Get Inside the Hacker's Mind→

