Hex Package Manager Reports Server Compromise; Users Told to Reset Credentials



Hex, the Elixir and Erlang package manager, says attackers executed commands on its web servers through a critical flaw. No package tampering was found, but database exposure cannot be ruled out, and users should reset passwords and 2FA.

- On November 23, attackers exploited an unauthenticated deserialization flaw (CVE-2026-129514, CVSS 10) in hex.pm to run OS commands.
- Hex says the attack was blocked and the defect fixed within 20 minutes; 69 malicious requests hit six web servers.
- No evidence of package modification, database changes or persistent access, but exposure of emails, password hashes, API key hashes, sessions and 2FA secrets cannot be excluded.
- Hex rotated storage, CDN, email and database credentials and signing keys, logging all users out.

> - The same class of flaw was patched in Ash Framework, db_connection and flop.

What happened

Hex, the package manager for Elixir and Erlang, disclosed that attackers gained unauthorized access to its web servers on November 23. They exploited an unauthenticated deserialization of untrusted data flaw in hex.pm, tracked as CVE-2026-129514 with a CVSS score of 10, using a crafted Erlang external term format request body to achieve remote code execution.

Between 18:16 and 18:29 UTC the attacker sent 69 malicious requests affecting six web servers. Hex replaced all servers with patched versions at 18:30, and a firewall rule fully blocked the attacker's traffic at 18:33.

What is and is not known

Hex reports no evidence of unauthorized package modification, database changes or lasting attacker access. However, it cannot rule out access to database contents, including email addresses, password hashes, API key hashes, sessions, second-factor secrets and audit logs. Reads from a compromised server would look legitimate, and database and private documentation reads are not logged, which limits visibility.

Because the commands could read server credentials, Hex replaced its storage, CDN, email and database credentials as well as session and token signing keys. All users were logged out of hex.pm and Hex clients.

The same class of flaw affected Ash Framework, patched on November 24 under CVE-2026-124283, and related defects were fixed in db_connection (CVE-2026-129514 is Hex only; db_connection is CVE-2026-133555) and flop (CVE-2026-130411).

Guidance from Hex

Account holders should change their hex.pm passwords and reset two-factor authentication. Until new client versions arrive, users should fetch packages only from repo.hex.pm and avoid third-party mirrors. Emails claiming to be from Hex deserve caution; confirm links lead to hex.pm.

What to do now

1. Identify Elixir/Erlang projects and CI/CD pipelines that use Hex, and confirm which accounts and API keys belong to your organization.
2. Have all hex.pm account holders change passwords and reset two-factor authentication, and rotate any Hex API keys as a precaution.
3. Restrict package fetching to repo.hex.pm and block third-party mirrors until updated Hex clients are released.
4. Update Ash Framework, db_connection and flop to patched versions and review code for unsafe deserialization of untrusted input.

5. Warn staff about phishing emails posing as Hex and require links to be checked against hex.pm.
6. If personal data may be affected, assess obligations under PDPL and your internal incident procedures.