hyperledger / **besu-native** Public

Code | Issues 4 | Pull requests 2 | Actions | **Security** 1 | Insights

ALTBN128_ADD, ALTBN128_MUL, ALTBN128_PAIRING precompile functions do not check if points are on curve

Critical **garyschulte** published **GHSA-jcp8-gh74-97hq** yesterday

Package	Affected versions	Patched versions
besu (Ethereum)	24.7.1 - 25.2.2	25.3.0
besu-native (Ethereum)	0.9.0 - 1.2.1	1.3.0

Severity

Critical

CVE ID

CVE-2025-30147

Weaknesses

No CWEs

Credits

asanso Finder

kevaundray Remediation reviewe

Description

Impact

All versions of Besu since 24.7.1 have a potential consensus bug for the precompiles:

- ALTBN128_ADD (0x06)
- ALTBN128_MUL (0x07)
- ALTBN128_PAIRING (0x08)

These precompiles were reimplemented in besu-native using gnark-crypto's bn254 implementation, as the former implementation used a library which was no longer maintained and not sufficiently performant. The new gnark implementation was initially added in version 0.9.0 of besu-native but was not utilized by besu until version 0.9.2 in besu 24.7.1.

The issue is that there are EC points which may be crafted which are in the correct subgroup but are not on the curve and the besu-native gnark implementation was relying on subgroup checks to perform point-on-curve checks as well. The version of gnark-crypto used at the time did not do this check when performing subgroup checks.

The result is that it was possible for besu to give an incorrect result and fall out of consensus when executing one of these precompiles against a specially crafted input point.

Additionally, homogenous Besu-only networks can potentially enshrine invalid state which would be incorrect and difficult to process with patched versions of besu which handle these calls correctly.

Patches

The underlying defect has been patched in besu-native release 1.3.0.
The fixed version of besu is version 25.3.0.

Workarounds

For versions of besu with the problem, the native precompile for altbn128 may be disabled in favor of the pure-java implementation. The pure java implementation is significantly slower, but does not have this consensus issue.

To disable the native precompile implementation on affected versions of besu, use this flag: `--Xaltbn128-native-enabled=false`

References

If you have any questions or comments about this advisory:

- Open an issue in Besu
- Email us at security@hyperledger.org