Signature forgery in Biscuit 1.0

Critical **Geal** published **GHSA-75rw-34q6-72cr** on Jun 11

Package

biscuit-auth (Rust)

Affected versions	Patched versions
1.0.0 to 1.1.0	2.0.0

biscuit-haskell (Haskell)

0.1.1.0	0.2.0.0

com.clever-cloud.biscuit-java (Maven)

<2.0.0	2.0.0

https://github.com/biscuit-auth/biscuit-go (Go)

<2.0	v2.0

Description

Impact

The paper Cryptanalysis of Aggregate Γ-Signature and Practical Countermeasures in Application to Bitcoin defines a way to forge valid Γ-signatures, an algorithm that is used in the Biscuit specification version 1.
It would allow an attacker to create a token with any access level.

As Biscuit v1 was still an early version and not broadly deployed, we were able to contact all known users of Biscuit v1 and help them migrate to Biscuit v2.
We are not aware of any active exploitation of this vulnerability.

Patches

The version 2 of the specification mandates a different algorithm than gamma signatures and as such is not affected by this vulnerability. The Biscuit implementations in Rust, Haskell, Go, Java and Javascript all have published versions following the v2 specification.

Workarounds

There is no known workaround, any use of Biscuit v1 should be migrated to v2.

References

Cryptanalysis of Aggregate Γ-Signature and Practical Countermeasures in Application to Bitcoin

For more information

If you have any questions or comments about this advisory:

- Open an issue in biscuit-auth/biscuit
- Ask questions on Matrix

Severity

Critical

CVE ID

CVE-2022-31053

Weaknesses

CWE-347