Mod security sandbox escape

Critical **sfan5** published **GHSA-g596-mf82-w8c3** yesterday

Package

No package listed

Affected versions

>= 5.0.0

Patched versions

5.15.2 or newer

Description

Impact

A malicious mod can trivially escape the sandboxed Lua environment to execute arbitrary code and gain full filesystem access on the user's device.
This applies to the server-side mod, async and mapgen as well as the client-side (CSM) environments.

This vulnerability is **only** exploitable when using LuaJIT. You can use `luanti --version` to determine the type of Lua in use.

Patches

`8a929df`

Workarounds

On release versions you can also patch this issue without recompiling by editing `builtin/init.lua` and adding the following line at the end:

```
getfenv = nil
```

Note that this will break mods relying on this function (which is not inherently unsafe).

References

–

Severity

Critical

CVE ID

No known CVE

Weaknesses

No CWEs