external calls are not clamped in certain complex expressions

High **charles-cooper** published **GHSA-j2x6-9323-fp7h** on Apr 13

Package

vyper (pip)

Affected versions	Patched versions
<0.3.2	0.3.2

Description

Impact

in the following code, the return of `<iface>.returns_int128()` is not validated to fall within the bounds of `int128`. as of v0.3.0, `<iface>.returns_int128()` is validated in simple expressions, but not complex expressions.

```
interface iface:
    def returns_int128() -> int128: view
    def returns_Bytes33() -> Bytes[33]: view

x: iface

@external
def call_out():
    x: int128 = self.x.returns_int128()  # affected, <0.3.0
    y: uint256 = convert(self.x.returns_int128(), uint256)  # affected, <0.3.2
    z: Bytes[33] = concat(self.x.returns_Bytes33(), b"")  # affected >= 0.3.0, <0.3.2
```

Patches

0.3.2 (as of `049dbdc`)

Workarounds

Break up operations involving external calls into multiple statements. For instance, instead of the example above, use

```
x: int128 = self.x.returns_int128()
y: uint256 = convert(x, uint256)
```

Severity

High

CVE ID

CVE-2022-24845

Weaknesses

No CWEs