Denial of Service in uap-core <=0.7.2 when processing crafted User-Agent strings

High **commenthol** published **GHSA-cmcx-xhr8-3w9p** on Feb 20, 2020

Package

uap-core (npm)

Affected versions	Patched versions
<=0.7.2	0.7.3

Description

Impact

Some regexes are vulnerable to regular expression denial of service (REDoS) due to overlapping capture groups. This allows remote attackers to overload a server by setting the User-Agent header in an HTTP(S) request to maliciously crafted long strings.

Patches

Please update uap-core to >= v0.7.3

Downstream packages such as uap-python, uap-ruby etc which depend upon uap-core follow different version schemes.

Details

Each vulnerable regular expression reported here contains 3 overlapping capture groups. Backtracking has approximately cubic time complexity with respect to the length of the user-agent string.

Regex 1:

```
\bSmartWatch *\( *([^;]+) *; *([^;]+) *;
```

is vulnerable in portion `*([^;]+) *` and can be attacked with

```
"SmartWatch(" + (" " * 3500) + "z"
```

e.g.

```
SmartWatch(                                  z
```

Regex 2:

```
; *([^;/]+) Build[/ ]Huawei(MT1-U06|[A-Z]+\d+[^\);]+)[^\);]*\)
```

is vulnerable in portion `\d+[^\);]+[^\);]*` and can be attacked with

```
";A Build HuaweiA" + ("4" * 3500) + "z"
```

Regex 3:

```
(HbbTV)/[0-9]+\.[0-9]+\.[0-9]+ \([^;]*; *(LG)E *; *([^;]*) *;[^;]*;[^;]*;\)
```

is vulnerable in portion `*([^;]*) *` and can be attacked with

```
"HbbTV/0.0.0 (;LGE;" + (" " * 3500) + "z"
```

Regex 4:

```
(HbbTV)/[0-9]+\.[0-9]+\.[0-9]+ \([^;]*; *(?:CUS:([^;]*)|([^;]+)) *; *([^;]*) *;.*;
```

is vulnerable in portions `*(?:CUS:([^;]*)|([^;]+)) *` and `*([^;]*) *` and can be attacked with

```
"HbbTV/0.0.0 (;CUS:;" + (" " * 3500) + "z"
"HbbTV/0.0.0 (;" + (" " * 3500) + "z"
"HbbTV/0.0.0 (;z;" + (" " * 3500) + "z"
```

Reported by Ben Caller **@bcaller**

Severity

High

CVE ID

CVE-2020-5243

Weaknesses

No CWEs

Credits

 bcaller