ADVISORY

DATE

6 AUGUST 2021

Corero SecureWatch Managed Services 9.7.2.0020 get_snapshot Path Traversal

Corero SecureWatch Managed Services 9.7.2.0020 is affected by a Path Traversal vulnerability via the `snap_file` parameter in the `/it-IT/splunkd/__raw/services/get_snapshot` HTTP API endpoint. A 'low privileged' attacker can read any file on the target host.

Product Description (from vendor)

"SecureWatch Managed Services are a comprehensive suite of configuration optimization, monitoring and mitigation response services. This round-the-clock service, delivered by Corero's highly experienced Security Operations Center, is tailored to meet the security policy requirements and business goals of each SmartWall customer that engages in a SecureWatch managed service plan." More information is available at https://www.corero.com/product/managed-ddos-protection-services/

CVE

- CVE-2021-38136

Root Cause Analysis

The file `/opt/splunk/etc/apps/securewatch_analytics_tdd/bin/snapshot_handler/snapshotHandler.py`, reachable via a HTTP request to `/it-IT/splunkd/__raw/services/get_snapshot`, uses the "snap_file" parameter to build the path of file to provide inside the HTTP response, without sanitizing the user input in any way.

```
class GetSnapshot(splunk.rest.BaseRestHandler):
    def handle_GET(self):

        try:
            snap_file = unquote(self.request['query']['snap_file'])
            with open('/corero/snapshots/' + snap_file, mode='rb') as file:
                fileContent = file.read()

        except IOError as e:
            logging.error("command '{}' return with error (code {}) {}".format(e.cmd, e.returncode, e.output))
            raise cherrypy.HTTPError(500, "Error while reading snapshot:{}".format(e.strerror))

        self.response.headers["Content-Type"] = 'application/octet-stream'
        self.response.write(fileContent)
```

By traversing the `/corero/snapshots/` path it is possible to read any file on the target host.

Proof of Concept

1. Log-in Corero Firewall with a user with "swa-monitor" privileges
2. Visit the following URL: https://$host/it-IT/splunkd/__raw/services/get_snapshot?snap_file=../../../../../../../../../../etc/shadow
3. Notice the content of the /etc/shadow file in the server response

Impact

An attacker with access to an account having 'swa-monitor' privileges can read the contents of any file on the target host.

Remediation

Upgrade Corero SecureWatch Managed Services to version 9.7.5 or later. (Note: we didn't verify the patch.)

Disclosure Timeline

- 01/12/2020: The vulnerability is found during an assessment for a Shielder client and reported to the vendor
- 09/12/2020: The vendor fixes the vulnerability with the release of Corero SecureWatch Managed Services version 9.7.5
- 06/08/2021: Shielder's advisory is made public

Credits

Giulio `linset` Casciaro from Shielder

This advisory was first published on https://www.shielder.com/advisories/corero_secure_watch_managed_services-get_snapshot-path-traversal/

INFO

Shielder S.r.l.

P.I. 11435310013

REA TO - 1213132

Registered Capital: 81.000,00 €

Via Palestro, 1/C
10064 Pinerolo (TO) Italy

CONTACTS

info@shielder.com

Landline: (+39) 0121 - 39 36 42

Commercial: (+39) 345 - 30 31 983

Technical: (+39) 393 - 16 66 814

Disclosure policy

Privacy policy