SEC Consult SA-20201002-0 :: Multiple Vulnerabilities in SevOne Network Management System (NMS)

From: SEC Consult Vulnerability Lab <research () sec-consult com>
Date: Fri, 2 Oct 2020 18:20:02 +0000

```
SEC Consult Vulnerability Lab Security Advisory < 20201002-0 >
=======================================================================
             title: Multiple Vulnerabilities
           product: SevOne Network Management System (NMS)
 vulnerable version: 5.7.2.22
      fixed version:
         CVE number:
            impact: Critical
          homepage: https://www.sevone.com/
             found: 2020-07-16
                by: Calvin Phang (Office Singapore)
                    SEC Consult Vulnerability Lab

                    An integrated part of SEC Consult
                    Europe | Asia | North America

                    https://www.sec-consult.com

=======================================================================

Vendor description:
-------------------
"SevOne provides modern monitoring and analytics solutions that organizations
need to monitor their networks today, tomorrow and beyond. SevOne simplifies
the extraction and enrichment of metric, flow, and streaming telemetry data
across multi-vendor networks enabling enterprises, carriers and managed services
providers to ensure optimal network operations and performance."

Source: https://www.sevone.com/company/about-us/


Business recommendation:
------------------------
The vendor did not respond to our communication attempts, hence no patch is
available. It's recommended to closely monitor any activities related to NMS.

An in-depth security analysis performed by security professionals is highly
advised, as the software may be affected from further security issues.


Vulnerability overview/description:
-----------------------------------
In order to exploit the identified security issues an attacker needs at
least the following privileges: "view alerts and manage devices"
depending on the role assigned.

1) Command Injection in Traceroute Feature (Authenticated User)
There is a command injection vulnerability found in "traceroute.php".
Any OS command can be injected by an authenticated user who has access to
the "SNMP Walk" page. This could lead to a full system compromise.

2) Multiple SQL Injection vulnerabilities (Authenticated User)
Due to insufficient input validation, the application allows the injection
of direct SQL commands. The identified SQL Injection vulnerabilities can
be exploited by an authenticated user who has access to the "Alert Summary"
and "Alert Archive" pages.

3) CSV Formula Injection vulnerability (Authenticated User)
The "Device Manager" page of the application has a "CSV export all devices"
feature which allows the export of device data (name, device IP, objects,
and so on) as a CSV file. On the "Device Creator" page, it is possible to
input a malicious formula that will be embedded inside an exported CSV file.
This vulnerability can be exploited by an authenticated user who has access to
the "Device Creator" page.


Proof of concept:
-----------------
PoC has been removed as no patch is available and the vendor is unresponsive.


Vulnerable / tested versions:
-----------------------------
SevOne Network Management System (NMS) version 5.7.2.22 has been tested.
Previous versions may also be affected.


Vendor contact timeline:
------------------------
2020-08-04: Contacting vendor through infosec-cases () sevone com; no response
2020-08-12: Follow-up with vendor; no response
2020-08-26: Follow-up with vendor; no response
2020-09-14: Follow-up with vendor; no response
2020-10-02: Public release of the security advisory


Solution:
---------
The vendor did not respond to our communication attempts, hence no patch is
available.


Workaround:
-----------
None


Advisory URL:
-------------
https://www.sec-consult.com/en/vulnerability-lab/advisories/index.html


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

SEC Consult Vulnerability Lab

SEC Consult
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult. It
```

ensures the continued knowledge gain of SEC Consult in the field of network
and application security to stay ahead of the attacker. The SEC Consult
Vulnerability Lab supports high-quality penetration testing and the evaluation
of new offensive and defensive technologies for our customers. Hence our
customers obtain the most current information about vulnerabilities and valid
recommendation about the risk profile of new technologies.

~~~~~~
Interested to work with the experts of SEC Consult?
Send us your application https://www.sec-consult.com/en/career/index.html

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://www.sec-consult.com/en/contact/index.html
~~~~~~

Mail: research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF C. Phang / @2020

By Date By Thread

Current thread:

SEC Consult SA-20201002-0 :: Multiple Vulnerabilities in SevOne Network Management System (NMS) ***SEC Consult Vulnerability Lab (Oct 02)***