

Securiteam: [NEWS] Nokia SGSN (DX200 Based Network Element) SNMP issue

# [NEWS] Nokia SGSN (DX200 Based Network Element) SNMP issue

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0039.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 03/16/03

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 16 Mar 2003 21:20:28 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or [ussales@beyondsecurity.com](mailto:ussales@beyondsecurity.com)

-----

Nokia SGSN (DX200 Based Network Element) SNMP issue

---

## SUMMARY

<<http://www.nokia.com>> Nokia's SGSN (Serving GPRS support node) is the platform that exists between the legacy GSM network and the new IP core of the GPRS network. This enables operators to deploy high-speed data access over the top of their GSM network with minimal upgrades to their BSCs (Base Station Controllers), thus making the transition from a 2.0G to a 2.5G network.

Due to its position in the network (i.e. between the RF network and the IP network), the SGSN will have interfaces on the SS7 signaling network and the IP core network as well as connections to the BSCs. For this reason, the SGSN can be considered a key part of the infrastructure of any mobile operator looking to deploy GPRS.

A vulnerability exists in the SNMP (Simple Network Management Protocol) daemon of the DX200 based network element that allows an attacker to read SNMP options with ANY community string.

## Securiteam: [NEWS] Nokia SGSN (DX200 Based Network Element) SNMP issue

This is a good example of why network elements that introduce IP functionality to legacy networks should have their functionality verified in terms of impact on security before deployment in a production environment.

### DETAILS

Vulnerable systems:

- \* Nokia SGSN (DX200 Based Network Element)

Proof of Concept:

The following proof of concept will return the default MIB information on the DX200 based network element using the snmpwalk and snmpset commands that ship by default with operating systems such as Linux.

[reading of SNMP details]

```
snmpwalk <IP of SGSN> tellmeyoursecrets
```

Vendor Response:

In SNMP v1 (RFC 1157) and v2c (RFC 1901) standards, authentication is based on a community string (text string) representing an unencrypted username without a password. A recognized concern in industry is that the security check as documented in these SNMP standards is inadequate.

Because of the above, read access to MIB-II (RFC 1213) variables is allowed in Nokia SGSN SG1 / SG1.5 products with any community string value. However, write access to MIB-II variables is not permitted in Nokia SGSN SG1 / SG1.5 products, even though the SNMP MIB-II RFC standard defines some of the MIB-II variables to be write accessible. Nokia has made a product design decision that the value of each write accessible MIB-II variable remains unchanged, even in cases where the SNMP agent in Nokia SGSN SG1 / SG1.5 products would return an OK status notification as a response to the SNMP set-request operation.

This means that a malicious attacker is under no circumstances able to alter any settings of Nokia SGSN SG1 / SG1.5 products via the SNMP interface. Furthermore, support for the SNMP interface has been removed from subsequent Nokia SGSN releases, which eliminates the possibilities for SNMP based vulnerabilities.

Vendor Recommendation:

Network operators do not need to take any further action.

@stake Recommendation:

Typically, in a GPRS network design, the SGSN should not be contactable from the Gi interface of the GGSN where the user's routable IP is located. This is because GGSN to SGSN communication occurs over the Gn interface. However, @stake has observed instances where the NMS (Network Management System) network is routable from the Gi network. If the SGSN has an NMS connection, then appropriate ACLs (Access Control Lists) should be deployed on the routing device or firewall between the Gi and the NMS

Securiteam: [NEWS] Nokia SGSN (DX200 Based Network Element) SNMP issue

networks to restrict access to SNMP.

ADDITIONAL INFORMATION

The original advisory can be downloaded by going to:

<[www.atstake.com/research/advisories/2003/a031303-2.txt](http://www.atstake.com/research/advisories/2003/a031303-2.txt)>

[www.atstake.com/research/advisories/2003/a031303-2.txt](http://www.atstake.com/research/advisories/2003/a031303-2.txt)

The information has been provided by <<mailto:ollie@atstake.com>> Ollie Whitehouse of @Stake.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.