

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

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-03/0024.html>

From: @stake Advisories (@stake)

Date: 03/13/03

Date: Thu, 13 Mar 2003 11:43:42 -0500

From: "@stake Advisories" <advisories@atstake.com>

To: vulnwatch@vulnwatch.org

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

@stake, Inc.
www.atstake.com

Security Advisory

Advisory Name: Nokia SGSN (DX200 Based Network Element) SNMP issue

Release Date: 03/13/2003

Application: Nokia SGSN (DX200 Based Network Element)

Platform: DX200

Severity: An attacker is able to read SNMP options with any community string

Author: Ollie Whitehouse [ollie@atstake.com]

Vendor Status: Vendor has removed support for this protocol

CVE Candidate: CVE Candidate number applied for

Reference: www.atstake.com/research/advisories/2003/a031303-2.txt

Overview:

Nokia's (<http://www.nokia.com>) SGSN (Serving GPRS support node) is the platform which 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

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

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.

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

Proof of Concept:

The following proof of concept will return the the default MIB information on the DX200 based network element using the snmpwalk and snmpset commands which 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 completely.

Vendor Recommendation:

Network operators do not need to take any further action.

@stake Recommendation:

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

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 due to the fact that 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 networks to restrict access to SNMP.

Common Vulnerabilities and Exposures (CVE) Information:

The Common Vulnerabilities and Exposures (CVE) project has assigned the following names to these issues. These are candidates for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

CVE Candidate number applied for

@stake Vulnerability Reporting Policy:
<http://www.atstake.com/research/policy/>

@stake Advisory Archive:
<http://www.atstake.com/research/advisories/>

PGP Key:
http://www.atstake.com/research/pgp_key.asc

@stake is currently seeking application security experts to fill several consulting positions. Applicants should have strong application development skills and be able to perform application security design reviews, code reviews, and application penetration testing. Please send resumes to jobs@atstake.com.

Copyright 2003 @stake, Inc. All rights reserved.

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.0

iQA/AwUBPnC08Ue9kNIfAm4yEQJ2IQCdG44PU+tfe3xhPurBU/hv1245iywAoOho
IWZVyS+ZVjulNcEzeTQzbfcw
=a9sy

-----END PGP SIGNATURE-----