

# [NEWS] Nokia GGSN (IP650 Based) DoS

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0026.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 06/12/03

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

Date: 12 Jun 2003 01:46:26 +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

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team?

Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Learn more at <http://www.coresecurity.com/promos/site1>,  
or call 617-399-6980

-----  
Nokia GGSN (IP650 Based) DoS  
-----

## SUMMARY

<<http://www.nokia.com>> Nokia's GGSN (Gateway GPRS support node) is the platform that exists between Gn and Gi networks within a GPRS network.

There exists a vulnerability in the TCP stack that allows an attacker to cause the GGSN to kernel panic and shutdown. This potentially allows an attacker to crash all data connectivity within a GPRS based network.

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 GGSN (IP650 Based)

## Securiteam: [NEWS] Nokia GGSN (IP650 Based) DoS

This vulnerability is exploited by sending a malformed IP packet with a TCP option of 0xFF over a cellphone to the affected network.

### Recommendation:

@stake worked with Nokia to ensure that all affected operators were informed, upgraded, and only after this time did @stake agree to release this information to the public. There should be no action on the part of the operator required.

Below is the notice that was sent out by Nokia to their clients:

---[Nokia Notice]---

### NOKIA CUSTOMER CONFIDENTIAL, GGSN RELEASE 1 VULNERABILITY

Under exceptional circumstances, Nokia GGSN release 1 is potentially vulnerable to a "Denial of Service" style of attack from a malicious user equipped with a computer and a mobile phone. When the vulnerability is exploited, the GGSN restarts. There is no damage to the configuration, but some charging data may be lost. Changing a normal Access Point to tunneled (GRE or IP in IP) prevents the attacks from mobile user side.

The same applies for the Gi interface though routers and firewalls would normally drop this kind of packets. The problem has been detected and reported by @stake and has been reproduced by Nokia in collaboration with @stake. Nokia and @stake are jointly working to eliminate the problem.

This vulnerability is corrected in IPSO version 3.4 and all subsequent versions. Thus, GGSN release 2 is not vulnerable, GGSN release 1 is. Nokia advises all the customers still running GGSN release level 1 to upgrade on GGSN release level 2.

As an interim measure, operators can perform the following preventative configuration changes to their networks. Ensure that all IP packets with non-standard IP options are dropped by boarder firewalls on the Gi interface. Within the Gn network, ensure that the GTP aware firewall (if present) also drops all encapsulated IP packets with non-standard IP options. This may introduce latency however, it will mitigate against the attack until the patch has been fully deployed and tested.

Due to the severity of this vulnerability @stake has confirmed that they will not be releasing this information publicly on their research page (<http://www.atstake.com/research/>) until Nokia has confirmed that all affected operators have fully patched and tested all affected elements. However, @stake would ideally like to release this information no later than 1st June 2003.

Neither @stake nor Nokia are aware of this attack being used in the wild as it was discovered by @stake within a lab environment and subsequently tested on a number of operators for whom they have worked for.

---[End Nokia Notice]---

Securiteam: [NEWS] Nokia GGSN (IP650 Based) DoS

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<<http://www.atstake.com/research/advisories/2003/a060903-1.txt>>

<http://www.atstake.com/research/advisories/2003/a060903-1.txt>

The information has been provided by <<mailto:advisories@atstake.com>>

@stake Advisories.

=====

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.