

[NEWS] Enterasys Networks Multiple NetSight Products Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00019.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 8 Apr 2007 13:43:56 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Enterasys Networks Multiple NetSight Products Multiple Vulnerabilities

SUMMARY

<<http://www.enterasys.com/products/management/>> NetSight is "a graphical network management platform combining multiple products into one console". Multiple vulnerabilities exist within the TFTP and BOOTP server components of various Enterasys Networks NetSight products.

DETAILS

Vulnerable Systems:

- * TFTP and BOOTP component of the NetSight packages on the Windows XP and Windows 2000 platform are vulnerable.
- * NetSight Console 2.1
- * NetSight Inventory Manager 2.1
- * Previous versions of the products, and versions for other platforms, may also contain vulnerable code, however this has not been confirmed.

Immune Systems:

- * iDefense has confirmed that the following releases of Enterasys' NetSight products are no longer vulnerable.
- * NetSight Console 2.3.1 build 6

[NEWS] Enterasys Networks Multiple NetSight Products Multiple Vulnerabilities

* NetSight Inventory Manager 2.2.2 build 4

The TFTPDP server component of various Enterasys Networks NetSight products contains a buffer overflow in the file name portion of a request packet. By sending a request packet with a long file name, it is possible to cause an exploitable stack based buffer overflow.

The BOOTPD server component of various Enterasys Networks NetSight products fails to validate the "packet type" field of packets it receives. By sending a UDP packet with a an invalid "packet type" it is possible to cause an the server to exit.

These services typically run as an administrative user. As the services use the UDP protocol, the source address of packets could be spoofed. This may allow bypassing of some host based firewall rules designed to limit connections to trusted clients.

Workaround:

These services can be stopped and started from an icon in the system tray. It is recommended that they not be activated unless required. Restricting access to the services to trusted clients may not be a viable option, as the services use the UDP protocol, which an attacker can easily spoof.

Disclosure Timeline:

- * 08/16/2006 – Initial vendor notification
- * 08/16/2006 – Initial vendor response
- * 04/04/2007 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense.
The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=506>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=506>

=====

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@xxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====
=====

[NEWS] Enterasys Networks Multiple NetSight Products Multiple Vulnerabilities

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.