

[Fwd: CERT Advisory CA-2003-13 Multiple Vulnerabilities in Snort Preprocessors]

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-04/0024.html>

From: Christopher Nehren (apeiron@comcast.net)

Date: 04/17/03

Date: Thu, 17 Apr 2003 16:51:15 -0400
From: Christopher Nehren <apeiron@comcast.net>
To: security@freebsd.org

I figured that someone reading this list might want to take a look at the proceeding, considering that the version of Snort in FreeBSD ports -is- affected.

-----Forwarded Message-----

> *From:* CERT Advisory <cert-advisory@cert.org>
> *To:* cert-advisory@cert.org
> *Subject:* CERT Advisory CA-2003-13 Multiple Vulnerabilities in Snort Preprocessors
> *Date:* 17 Apr 2003 11:30:47 -0400
>
>
>
> -----BEGIN PGP SIGNED MESSAGE-----
>
> *CERT Advisory CA-2003-13 Multiple Vulnerabilities in Snort Preprocessors*
>
> *Original release date:* April 17, 2003
> *Last revised:* --
> *Source:* CERT/CC
>
> *A complete revision history can be found at the end of this file.*
>
> *Systems Affected*
>
> ** Snort IDS, versions 1.8 through 2.0 RC1*
>
> *Overview*
>
> *There are two vulnerabilities in the Snort Intrusion Detection System,*
> *each in a separate preprocessor module. Both vulnerabilities allow*
> *remote attackers to execute arbitrary code with the privileges of the*
> *user running Snort, typically root.*
>

> *I. Description*

>

> *The Snort intrusion detection system ships with a variety of
> preprocessor modules that allow the user to selectively include
> additional functionality. Researchers from two independent
> organizations have discovered vulnerabilities in two of these modules,
> the RPC preprocessor and the "stream4" TCP fragment reassembly
> preprocessor.*

>

> *For additional information regarding Snort, please see*

>

> *<http://www.snort.org/>.*

>

> *VU#139129 – Heap overflow in Snort "stream4" preprocessor (CAN–2003–0029)*

>

> *Researchers at CORE Security Technologies have discovered a remotely
> exploitable heap overflow in the Snort "stream4" preprocessor module.
> This module allows Snort to reassemble TCP packet fragments for
> further analysis.*

>

> *To exploit this vulnerability, an attacker must disrupt the state
> tracking mechanism of the preprocessor module by sending a series of
> packets with crafted sequence numbers. This causes the module to
> bypass a check for buffer overflow attempts and allows the attacker to
> insert arbitrary code into the heap.*

>

> *For additional information, please read the Core Security Technologies
> Advisory located at*

>

> *<http://www.coresecurity.com/common/showdoc.php?idx=313&idxseccion=10>*

>

> *This vulnerability affects Snort versions 1.8.x, 1.9.x, and 2.0 prior
> to RC1. Snort has published an advisory regarding this vulnerability;
> it is available at*

>

> *<http://www.snort.org/advisories/snort-2003-04-16-1.txt>.*

>

> *VU#916785 – Buffer overflow in Snort RPC preprocessor (CAN–2003–0033)*

>

> *Researchers at Internet Security Systems (ISS) have discovered a
> remotely exploitable buffer overflow in the Snort RPC preprocessor
> module. Martin Roesch, primary developer for Snort, described the
> vulnerability as follows:*

>

> *When the RPC decoder normalizes fragmented RPC records, it
> incorrectly checks the lengths of what is being normalized against
> the current packet size, leading to an overflow condition. The RPC
> preprocessor is enabled by default.*

>

> *For additional information, please read the ISS X–Force advisory
> located at*

- >
- > <http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21951>
- >
- > *This vulnerability affects Snort versions 1.8.x through 1.9.1 and*
- > *version 2.0 Beta.*
- >
- > *II. Impact*
- >
- > *Both VU#139129 and VU#916785 allow remote attackers to execute*
- > *arbitrary code with the privileges of the user running Snort,*
- > *typically root. In addition, it is not necessary for the attacker to*
- > *know the IP address of the Snort device they wish to attack; merely*
- > *sending malicious traffic where it can be observed by an affected*
- > *Snort sensor is sufficient to exploit these vulnerabilities.*
- >
- > *III. Solution*
- >
- > *Upgrade to Snort 2.0*
- >
- > *Both VU#139129 and VU#916785 are addressed in Snort version 2.0, which*
- > *is available at*
- >
- > <http://www.snort.org/dl/snort-2.0.0.tar.gz>
- >
- > *Binary-only versions of Snort are available from*
- >
- > <http://www.snort.org/dl/binaries>
- >
- > *For information from other vendors that ship affected versions of*
- > *Snort, please see Appendix A of this document.*
- >
- > *Disable affected preprocessor modules*
- >
- > *Sites that are unable to immediately upgrade affected Snort sensors*
- > *may prevent exploitation of this vulnerability by commenting out the*
- > *affected preprocessor modules in the "snort.conf" configuration file.*
- >
- > *To prevent exploitation of VU#139129, comment out the following line:*
- >
- > *preprocessor stream4_reassemble*
- >
- > *To prevent exploitation of VU#916785, comment out the following line:*
- >
- > *preprocessor rpc_decode: 111 32771*
- >
- > *After commenting out the affected modules, send a SIGHUP signal to the*
- > *affected Snort process to update the configuration. Note that*
- > *disabling these modules may have adverse affects on a sensor's ability*
- > *to correctly process RPC record fragments and TCP packet fragments. In*
- > *particular, disabling the "stream4" preprocessor module will prevent*
- > *the Snort sensor from detecting a variety of IDS evasion attacks.*

- >
- > *Block outbound packets from Snort IDS systems*
- >
- > *You may be able limit an attacker's capabilities if the system is*
- > *compromised by blocking all outbound traffic from the Snort sensor.*
- > *While this workaround will not prevent exploitation of the*
- > *vulnerability, it may make it more difficult for the attacker to*
- > *create a useful exploit.*
- >
- > *Appendix A. – Vendor Information*
- >
- > *This appendix contains information provided by vendors for this*
- > *advisory. As vendors report new information to the CERT/CC, we will*
- > *update this section and note the changes in our revision history. If a*
- > *particular vendor is not listed below, we have not received their*
- > *comments.*
- >
- > *Apple Computer, Inc.*
- >
- > *Snort is not shipped with Mac OS X or Mac OS X Server.*
- >
- > *Ingrian Networks*
- >
- > *Ingrian Networks products are not susceptible to VU#139129 and*
- > *VU#916785 since they do not use Snort.*
- >
- > *Ingrian customers who are using the IDS Extender Service Engine to*
- > *mirror cleartext data to a Snort–based IDS should upgrade their IDS*
- > *software.*
- >
- > *NetBSD*
- >
- > *NetBSD does not include snort in the base system.*
- >
- > *Snort is available from the 3rd party software system, pkgsrc. Users*
- > *who have installed net/snort, net/snort–mysql or net/snort–pgsql*
- > *should update to a fixed version. pkgsrc/security/audit–packages can*
- > *be used to keep up to date with these types of issues.*
- >
- > *Red Hat Inc.*
- >
- > *Not vulnerable. Red Hat does not ship Snort in any of our supported*
- > *products.*
- >
- > *SGI*
- >
- > *SGI does not ship snort as part of IRIX.*
- >
- > *Snort*
- >
- > *Snort 2.0 has undergone an external third party professional security*

> *audit funded by Sourcefire.*

>

>

> *The CERT/CC acknowledges Bruce Leidl, Juan Pablo Martinez Kuhn, and
> Alejandro David Weil of Core Security Technologies for their discovery
> of VU#139129. We also acknowledge Mark Dowd and Neel Mehta of ISS
> X–Force for their discovery of VU#916785.*

>

>

> *Authors: Jeffrey P. Lanza and Cory F. Cohen.*

>

>

> *This document is available from:*

> <http://www.cert.org/advisories/CA–2003–13.html>

>

>

> *CERT/CC Contact Information*

>

> *Email: cert@cert.org*

> *Phone: +1 412–268–7090 (24–hour hotline)*

> *Fax: +1 412–268–6989*

> *Postal address:*

> *CERT Coordination Center*

> *Software Engineering Institute*

> *Carnegie Mellon University*

> *Pittsburgh PA 15213–3890*

> *U.S.A.*

>

> *CERT/CC personnel answer the hotline 08:00–17:00 EST(GMT–5) /*

> *EDT(GMT–4) Monday through Friday; they are on call for emergencies*

> *during other hours, on U.S. holidays, and on weekends.*

>

> *Using encryption*

>

> *We strongly urge you to encrypt sensitive information sent by email.*

> *Our public PGP key is available from*

> http://www.cert.org/CERT_PGP.key

>

> *If you prefer to use DES, please call the CERT hotline for more*

> *information.*

>

> *Getting security information*

>

> *CERT publications and other security information are available from*

> *our web site*

> <http://www.cert.org/>

>

> *To subscribe to the CERT mailing list for advisories and bulletins,*

> *send email to majordomo@cert.org. Please include in the body of your*

> *message*

>

> *subscribe cert–advisory*
>
> * "CERT" and "CERT Coordination Center" are registered in the U.S.
> Patent and Trademark Office.
>

>
> **NO WARRANTY**
> Any material furnished by Carnegie Mellon University and the Software
> Engineering Institute is furnished on an "as is" basis. Carnegie
> Mellon University makes no warranties of any kind, either expressed or
> implied as to any matter including, but not limited to, warranty of
> fitness for a particular purpose or merchantability, exclusivity or
> results obtained from use of the material. Carnegie Mellon University
> does not make any warranty of any kind with respect to freedom from
> patent, trademark, or copyright infringement.
>

>
> *Conditions for use, disclaimers, and sponsorship information*
>
> *Copyright 2003 Carnegie Mellon University.*
>
> *Revision History*
> *April 17, 2003: Initial release*
>
> -----BEGIN PGP SIGNATURE-----
> Version: PGP 6.5.8
>
> iQCVAwUBPp7GWGjtSoHZUTs5AQGmlAP+MWnegmA1Qft9AenH7xefffpEDVGDT+sl
> T4iljwl/ySozE962r40mLAKCszZDPdwRW/MyMA7ZcFaoWbiZc/QRhTa4A/YYJWC
> A4kL1cEnM/LiQ7yYBSnJ6DIWDT0+M1PUS9so02M6a0f0e4jzXZDJ5HmPDdo/aPq
> NW70cU8gbgs=
> =Vs2Q
> -----END PGP SIGNATURE-----

-
- application/pgp–signature attachment: [This is a digitally signed message part](#)