

Re: Syslog date/time format

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-sun/2001-12/0005.html>

From: Crist J. Clark (cristjc@earthlink.net)

Date: 12/05/01

Date: Wed, 5 Dec 2001 13:44:25 -0800
From: "Crist J. Clark" <cristjc@earthlink.net>
To: "Ogle Ron (Rennes)" <OgleR@thmulti.com>

On Wed, Dec 05, 2001 at 06:19:00PM +0100, Ogle Ron (Rennes) wrote:

- > *We are trying to create a centralized log repository for our *nix systems*
- > *mostly of Solaris persuasion. The problem is that these systems are located*
- > *around the globe in different time zones. We would like the central*
- > *repository to collect the logs using GMT/UTC time.*
- >
- > *When syslog on the local machine sends a message to the central repository,*
- > *it sends the message using it's own local time. This causes a problem when*
- > *trying to correlate data. We would like to change all entries in the*
- > *central repository to GMT/UTC time.*
- >
- > *It doesn't look like there are any switches available on the syslogd or*
- > *syslog.conf to make the local machine use GMT/UTC time instead of local time*
- > *for log entries. I'm currently looking at modifying the syslogd code to*
- > *allow for a switch that would allow the log program to use GMT/UTC time*
- > *instead of the local time.*
- >
- > *First, is this the right approach to use in changing syslogd?*

RFC3164 says that the `TIMESTAMP` is the source machine's local time. So this would actually break "the standard." But keep in mind RFC3164 is more of a documentation of how most syslogds currently work rather than a well thought out standard that was put down and the later syslogd implementations followed. (In hindsight, a UNIX epoch timestamp would be unambiguous and an even more simple data format to send.)

--
Crist J. Clark | cjclark@alum.mit.edu
| cjclark@jhu.edu
<http://people.freebsd.org/~cjc/> | cjc@freebsd.org

- **Previous message:** [Darren J Moffat: "Re: Syslog date/time format"](#)
- **In reply to:** [Ogle Ron \(Rennes\): "Syslog date/time format"](#)
- **Next in thread:** [Darren J Moffat: "Re: Syslog date/time format"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)