Symmetricom

2300 Orchard Parkway
San Jose, CA 95131-1017
Tel: (408) 433-0910

FIELD SERVICE BULLETIN

FSB #: 098-50620-029 **DATE: February 8th, 2010**

System: SyncServer S2xx and S3xx Series Network Time Servers

Product Identity: NTP Servers

Product Code: Description: CLEI Code: N/A

1520R-S300	SyncServer S300
1520R-S300-RB	SyncServer S300 with Rubidium Oscillator
1520R-S300-DC	SyncServer S300 & 40-60 VDC Power Supply
1520R-S300-RB-DC	SyncServer S300 & RB Oscillator & 40-60 VDC Power Supply
1520R-S350	SyncServer S350
1520R-S350-RB	SyncServer S350 with Rubidium Oscillator
1520R-S350-DC	SyncServer S350 & 40-60 VDC Power Supply
1520R-S350-RB-DC	SyncServer S350 & RB Oscillator & 40-60 VDC Power Supply
1520R-S200	SyncServer S200
1520R-S200-DC	SyncServer S200 & 40-60 VDC Power Supply
1520R-S250	SyncServer S250
1520R-S250-DC	SyncServer S250 & 40-60 VDC Power Supply
1520R-S250i	SyncServer S250i
1520R-S250i-DC	SyncServer S250i & 40-60 VDC Power Supply
1520-S200	SyncServer S200
1520-S200-DC	SyncServer S200 & 40-60 VDC Power Supply
1520-S200-RB	SyncServer S200 with Rubidium Oscillator
1520-S200-RB-DC	SyncServer S200 & Rubidium Oscillator & 40-60 VDC Power Supply
1520-S250	SyncServer S200
1520-S250-DC	SyncServer S200 & 40-60 VDC Power Supply
1520-S250-RB	SyncServer S250 with Rubidium Oscillator
1520-S250-RB-DC	SyncServer S250 & Rubidium Oscillator & 40-60 VDC Power Supply
1520-S250i	SyncServer S200
1520-S250i-DC	SyncServer S200 & 40-60 VDC Power Supply
1520-S250i-RB	SyncServer S250i with Rubidium Oscillator
1520-S250i-RB-DC	SyncServer S250i & Rubidium Oscillator & 40-60 VDC Power Supply

---

NOTE: Find a copy of this FSB in Support section of our website at http://www.symmetricom.com

Classification: National Vulnerability Database #CVE-2009-3563
US-CERT VU#568372

Behavior: NTP contains a vulnerability in the handling of mode 7 requests, which can result in a denial-of-service condition.

Summary: ntp_request.c in ntpd in NTP before 4.2.4p8, and 4.2.5, allows remote attackers to cause a denial of service (CPU and bandwidth consumption) by using MODE_PRIVATE to send a spoofed (1) request or (2) response packet that triggers a continuous exchange of MODE_PRIVATE error responses between two NTP daemons.

Description: NTP mode 7 (MODE_PRIVATE) is used by the ntpdc query and control utility. In contrast, ntpq uses NTP mode 6 (MODE_CONTROL), while routine NTP time transfers use modes 1 through 5.

Upon receipt of an incorrect mode 7 request or a mode 7 error response from an address which is not listed in a "restrict ... noquery" or "restrict ... ignore" statement, ntpd will reply with a mode 7 error response (and log a message).

In this case:

> If an attacker spoofs the source address of ntpd host A in a mode 7 response packet sent to ntpd host B, both A and B will continuously send each other error responses, for as long as those packets get through.
>
> If an attacker spoofs an address of ntpd host A in a mode 7 response packet sent to ntpd host A, A will respond to itself endlessly, consuming CPU and logging excessively.

Recommended Actions: None at this time

Permanent Solution: Symmetricom plans to release version 1.25 for the S2xx SyncServers and version 2.50 for the S3xx SyncServers that will eliminate this vulnerability. Upon the release of the software upgrade Symmetricom will issue a Product Change Notice (PCN). PCN's are available at: www.symmetricom.com.

In addition to the PCN, all SyncServers with Port 80 access to the Internet, and Update Notification enabled in the SyncServer will notify users of update availability, via email, SNMP trap, log file entry, and/or LED depending on user settings.

Contact Information:

Symmetricom Inc
3750 Westwind Blvd
Santa Rosa CA 95403

Toll Free Calls
888.367.7966 option 1, then option 2
Toll Calls
408-428-7907 (1) (2)
International Tech Support fax number
707.636.1891