

Quantum NOC77101 Firmware Release Notes



Exec Revision History

V1.07	4/1/2016	Problem fixed / Enhancement <ul style="list-style-type: none">• Removed a Remote Code Execution vulnerability in the websSecurityHandler (Advisory ICSA-15-351-01)• Removed a web server vulnerability to a remote file inclusion attack. (ICS-ALERT-15-224-02)• With version 1.06, the I/O Scanner would timeout before the server had a chance to respond. This behavior would not occur with version 1.02.• Resolves Java 1.8 issues.	Details <p>The 'Keep Alive' back-off algorithm was changed.</p>
V1.06	10/17/2014	Problem fixed / Enhancement <ul style="list-style-type: none">• After a power cycle event, there was a possibility that the NOC77101 could boot up with an incorrect MAC address.• When doing a full download to a PLC with a NOC77101 running I/O Scanner, the values read by the I/O Scanners on other NOC devices on the network may flicker.• The I/O Scanner Health bits do not reflect the state of the I/O Scanner on a cable pull from the 140NOC77101.	Details <p>The event, which caused a sector loss that contained the MAC address on bootup, was corrected.</p> <p>A connection management issue was resolved.</p> <p>The problem was resolved in identifying which state machines are active.</p>
V1.05	6/30/2014	Problem fixed / Enhancement <ul style="list-style-type: none">• In HTTP using directory traversals an attacker can bypass the basic authentication mechanism. Security Alert - ICS-VU-529542• Issue with Java Version 1.7. Files did not have Signature. The Java dialog box provides a warning indicating that this is a unsigned application.	Details <p>Checks have been put in so that this is no longer possible.</p> <p>The files all have been properly signed.</p>

		<ul style="list-style-type: none"> • Customers using the 140NOC77101 experiencing 12 minute recovery times if cable is pulled from the NOC after the first link is made. 	<p>The customer can use the MSTR block function 16 to close connections.</p>
V1.04	1/14/2013	<p>Problem fixed / Enhancement</p> <ul style="list-style-type: none"> • Fast Retransmission behavior is inconsistent with other products. The server requires three Duplicate ACKs to trigger fast retransmission behavior. It should initiate fast retransmission upon reception of a single duplicate ACK. • An improvement was made to in the switch driver code. 	<p>Details</p> <p>This has been corrected and the fast retransmission algorithm is triggered by a single Duplicate ACK.</p> <p>Changes made to how the driver selects which mode to use to communicate with the Marvel Switch for getting and setting of diagnostic and management data.</p>
V1.03	7/25/2012	<p>Problem fixed / Enhancement</p> <ul style="list-style-type: none"> • Execution of MSTR block while link is disconnected causes module to fault. A resource contention causes an access issue which could tie up the switch interface and require a reboot to clear. • Under certain rare conditions the module fails to power up. Certain PSX applications could cause power up issues with the NOC module. • There were various issues related to security. They include unencrypted passwords, open services that are insecure, multiple well-known passwords and an open debug port in the stack. 	<p>Details</p> <p>The contention was resolved by adjusting the priority for the tasks.</p> <p>These specific applications would create backplane behavior issues where the configuration was not read properly, resulting in a power up issue. Modification of the firmware corrects the backplane behavior and resolves the power up issue.</p> <ul style="list-style-type: none"> • Encrypted HTTP password file that is stored on file system. • Recompiled firmware without symbol table. • Removed unused logins/passwords from firmware. • Use encrypted passwords in the code. • Removed WindRiver debug port service. • Removed Telnet service
V1.02	Patch	<p>Problem fixed / Enhancement</p> <ul style="list-style-type: none"> • Communications would halt after approximately 50 days of continuous operation without indication to the user. A power cycle was required to recover communications. 	<p>Details</p> <p>The problem was due to the rollover of a set of counters which are used to determine the time of communications.</p>