Basecamp for Serial Converters

October 30, 2015 by Reid W — 3 Comments

Corey Thuen lead a recent Labs research project focused on Serial-to-Ethernet gateways.

Traditionally, remote field sites were connected to wide ICS and SCADA networks via serial connections. Leased serial lines are increasingly harder to come by, as telcos phase them out. Where they are still available, the support costs go up annually in order to price the lines out of existence. As a result most utilities are now forced to change over to IP-based networks for these remote systems, even when the basic control equipment is not being upgraded. In other cases, the serial device is working fine or has no suitable replacement, and the ICS operator wants to use their modern network to retrieve data from and send commands to a device.

Enter Serial to Ethernet converters. These devices allow utilities and other ICS operators to connect their old serial devices onto an Ethernet network. Features vary, but many devices feature virtual serial port drivers so that a standard server operating system such as Windows is lulled into believing that the device is plugged into a serial port. Other devices may support protocol translators, so that Modbus/TCP can be used on the Ethernet network to communicate with a serial Modbus device.

Labs performed an in-depth technical analysis of the top five vendors in the Serial to Ethernet converter space, and the results should not surprise anyone who paid attention to Project Basecamp. Tested vendors include big names like Moxa, Lantronix, Digi, and GridConnect.

Testing included searching for:

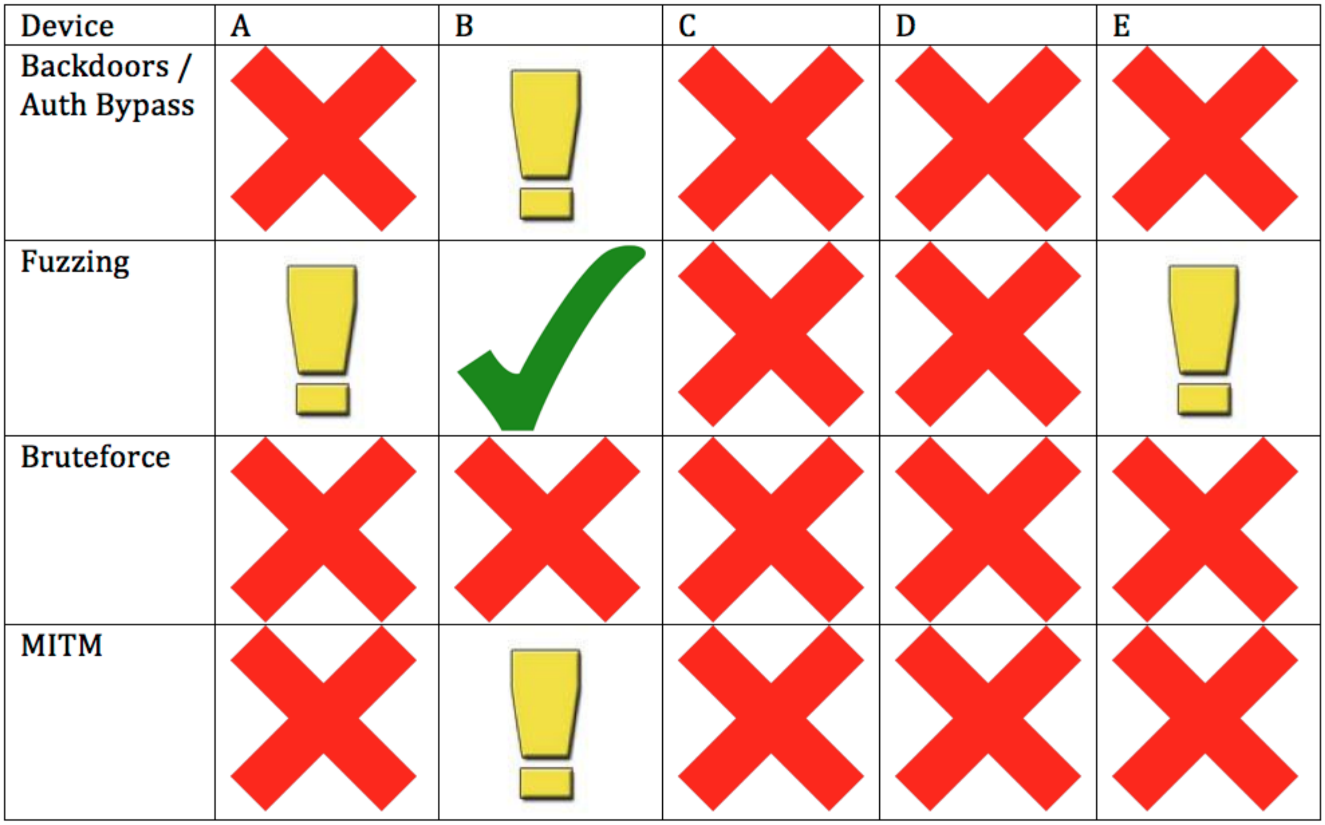
Backdoors into the device, including the ability to bypass authentication

Fuzz-testing issues, such as device crashing or rebooting on bad input

Bruteforce attacks against the device authentication systems

Man-in-the-middle attacks against the serial interface and management protocols

The results speak for themselves. We anonymized the results to protect the guilty, as it is obvious that none of the vendors are yet implementing a security process in their development lifecycle. Instead of saying which device is which, we simply labelled them ‘A’, ‘B’, ‘C’, ‘D’, and ‘E’.



Device	A	B	C	D	E
Backdoors / Auth Bypass	✗	!	✗	✗	✗
Fuzzing	!	✓	✗	✗	!
Bruteforce	✗	✗	✗	✗	✗
MITM	✗	!	✗	✗	✗

As with Basecamp, a red ‘X’ in a category indicates a catastrophic failure. The yellow exclamation mark ‘!’ means that a recoverable problem was found or that a partial compromise was possible, and a green checkmark indicates that the device passed the testing. Sadly we almost didn’t need the green check mark for this table.

Our original goal in the testing was just to perform a general pentest, applying a standard arsenal of techniques (and to hopefully learn a few things about encoding serial data over a TCP tunnel along the way). What fell out of testing were some eerie similarities between devices.

- Most devices use proprietary management protocols that either lack authentication for sensitive changes, or allow the end user to read (and in some cases even change) settings without authenticating first. For example, read the password if you understand the protocol.

- Most of the devices lacked even a correct IP stack implementation. Running open-source stack testing tools resulted in frequent reboots and crashes.
- Two of the devices were found to have an OEM relationship: identical hardware and very similar software were used in the (technically competing) products.
- One model, advertised as a 'high security' device by its vendor, allowed reading sensitive passwords from the device without authenticating first.
- None of the devices were secure by default, and most were insecure under any configuration.

While there was a 'winner' in the form of a device having fewer problems than others, even it has serious security issues.

Of course there are practical methods of securing devices, including both configuration hardening and network deployment guidelines. If you are an end user (or an affected vendor) and would like to read a full report specific to your device, contact us.

Filed Under: Basecamp, Control System IT, Feature, Research, Tools&Talks, Vulnerabilities, Vulnerability Disclosure
Tagged With: Basecamp, serial converters

Comments

Chris L says

October 30, 2015 at 12:24

Did you test any of DCB's products?

LT says

November 17, 2015 at 12:59