



TEST REPORT

CODIAN MCU 4200 SERIES & IP VCR 2200 SERIES VIDEO DEVICES



SEPTEMBER 2006



www.westcoastlabs.org

CONTENTS

CODIAN MCU 4200 SERIES & IP VCR 2200 SERIES VIDEO DEVICES CODIAN LIMITED



14 Waterside Drive, Langley, Slough SL3 6EZ, United Kingdom. Tel: +44 (0) 1753 548333

Test Lab & Vendor Details3

Executive Summary 4

Introduction and Objectives..... 5

Test Items..... 6

Test Equipment..... 7

Test Network - Diagram8

Test Methodology9

Test Results10

Conclusion 11

About Codian12

About West Coast Labs 13

West Coast Labs Standard Disclaimer 14



TEST LAB & VENDOR DETAILS

VENDOR DETAILS

Vendor Name: Codian Limited

Vendor Address: 14 Waterside Drive, Langley, Slough SL3 6EZ, United Kingdom

Vendor Telephone Number: +44 (0) 1753 548333

Product: Codian MCU 4200 Series and the IP VCR 2200 Series Video Firewalls

TEST LABORATORY DETAILS

Test Laboratory Name: West Coast Labs

Test Laboratory Address: William Knox House, Britannic Way, Llandarcy, Swansea, UK, SA10 9EL

Test Laboratory Telephone Number: +44 (0) 1792 324000

Date: September 2006

Issue: 1.0

Author: R Tanner

CONTACT POINTS FOR TECHNICAL QUERIES ON THE TEST REPORT

Contact Name: R Tanner

Contact Telephone Number: +44 (0) 1792 324000

EXECUTIVE SUMMARY

West Coast Labs independently defined and conducted an extensive range of comprehensive real-world tests – including TCP/IP based scans, probes and malformed packet injections – against the Codian MCU 4200 Series and the IP VCR 2200 Series of products, with a single key objective in mind; to detect any instances of disallowed, potentially malicious packet forwarding between the external and internal interfaces of each device under test.

Rigorous testing within specific, controlled conditions – performed both with and without active video conferencing sessions – confirmed that the Codian Video Firewall Feature for both the MCU and IP VCR products forwarded zero packets of any tested type, between the external and internal interfaces. This validates the robustness and intrinsic security of these products within a typical real-world deployment.

INTRODUCTION & OBJECTIVES



INTRODUCTION

Codian, a leader in the production of video conferencing infrastructure solutions request independent validation of a specific security claim relating to two of their core products. As a result, West Coast Labs (WCL) were engaged to autonomously test and ensure that – within specified parameters – this claim was accurate. Veridical attack vectors and common hacking techniques were utilized by WCL to help ensure the integrity of testing. Both the scope and the overall test results are published within this report.

OBJECTIVE

The single key objective of these tests was to evaluate the authenticity of a security claim made by Codian, regarding two of their devices. Specifically to validate that each device under test (DUT) would forward / route zero packets between the external and internal interfaces – with each DUT acting solely as an application layer bridge for video conferencing endpoints. Thus, helping to protect any connected networks from potentially malicious packet injections, that could conceivably be designed to compromise security in the real world.

TEST ITEMS



MCU 4200 SERIES

THE MCU 4200 SERIES AS DESCRIBED BY CODIAN:

“the most powerful conferencing bridge available, delivering the highest quality voice and video with an easy-to-use, versatile interface. Codian’s hardware MCU provides a rich multimedia experience with exceptional audio and visual clarity that makes it easy to communicate, collaborate and share data.”

IP VCR 2200 SERIES

THE IP VCR 2200 SERIES AS DESCRIBED BY CODIAN:

“a unique digital recorder specifically designed for video conferencing, enabling you to preserve valuable video content for future viewing. This innovative IP-based system records, streams live, or plays back on demand to a PC or any video conferencing endpoint. Codian’s IP VCR is flexible and exceptionally easy to install and operate. Use the Codian IP VCR for corporate training, executive briefings, web-casts, news, collaboration, distance learning, telemedicine and more.”

TEST EQUIPMENT



The test equipment comprised of an isolated computer network designed to mirror a typical real-world configuration, in which each DUT was individually deployed within the test network at separate times during the overall test cycle.

The test network - identically configured for each DUT – consisted of the following core components:

An external computer, able to view the public IP address that was preconfigured on port A – the external interface – of the DUT. This computer was set-up to emulate a video conferencing endpoint, connecting to the DUT via the simulated Internet.

A secondary external computer, able to view the public IP address that was preconfigured on port A – the external interface – of the DUT. This computer was set-up with the appropriate tools and technologies to emulate the machine of a real-world hacker. An additional arsenal of automated scripts, manually crafted packet captures and network-based Trojan malware samples were also available on this computer. Tools included firewall testing, port scanning, TCP/IP replaying and packet editing technologies.

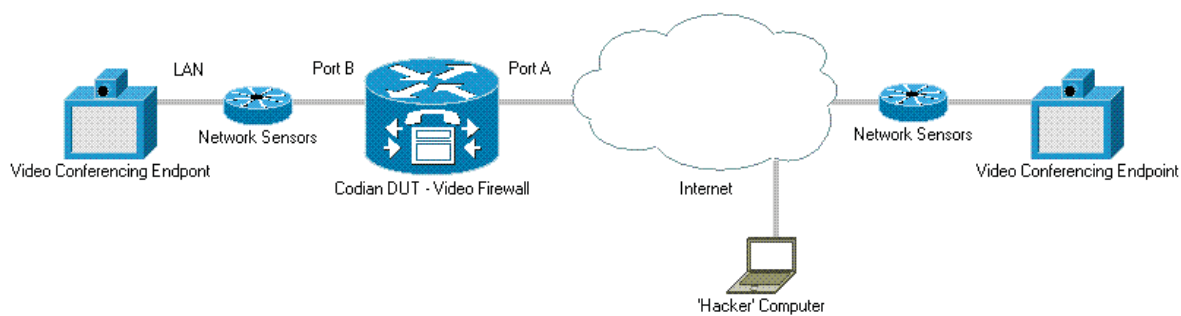
A tertiary external machine, able to view the public IP address that was preconfigured on port A – the external interface – of the DUT. This machine was used for monitoring purposes, having comprehensive network sensor, packet capturing, and protocol analysis capabilities.

An internal computer, able to view the private IP address that was preconfigured on port B – the internal interface – of the DUT. This computer was set-up to emulate a video conferencing endpoint, connecting to the DUT via the local area network.

A secondary internal machine, able to view the private IP address that was preconfigured on port B – the internal interface – of the DUT. This machine was used for monitoring and configuration purposes, having comprehensive network sensor, packet capturing, network disk imaging, and protocol analysis capabilities.

TEST NETWORK DIAGRAM

The following diagram is a high-level visual representation of the network used throughout the test process:



TEST METHODOLOGY



The test methodology defined and employed by WCL was identical for each DUT and was primarily chosen to address the needs of creating a measurement baseline, while ensuring the accurate detection of packets by network sensors and packet capturing technologies, in addition to considering how best to implement the available real-world TCP/IP based attack methods and payloads. The same methodology was utilized both with and without previously identified video conferencing traffic. The methodology and test process are outlined below:

Protocol analyzers, network sensors and packet capture tools were set-up to listen on the internal network – port B of the DUT. These components were tested and verified as working correctly. A secondary set of analyzers, sensors and capture tools were set-up to listen on the external network – port A of the DUT – to detect any disallowed outbound connection attempts.

A baseline image of the hard disk drive, in the internal 'video conferencing endpoint' was saved and transferred via the network to the internal 'monitoring' machine.

For initial reconnaissance, a number of commercially available, proprietary and open-source port scanners and network probing utilities were activated – from the external 'hacker' computer – to passively identify the status of all ports on the public IP address of the DUT. Multiple scanners and probes were used and all results compared, to ensure an accurate analysis of port status on the DUT. The results were further validated by manual confirmation of port status on the DUT itself.

Proprietary, commercial and open-source test scripts, software and hardware were configured to attack the DUT – from the external 'hacker' computer – on all verified open ports plus a random range of verified closed and / or stealth ports. Packets were both automatically and manually crafted and deployed. A manually edited traffic capture file containing various Trojan malware samples was also introduced.

A secondary image of the hard disk drive, in the internal 'video conferencing endpoint' was saved and transferred via the network to the internal 'monitoring' machine.

All protocol analyzer, network sensor and packet capture logs were manually analyzed to detect disallowed packet transfers, then the baseline and secondary images were compared to detect prohibited Trojan file transfers.

TEST RESULTS

Zero manufactured, malicious packets were detected traversing from the external to the internal interface, throughout testing.

A total of 200,007 TCP/IP-based tests were performed – automated and manual – including malformed packet injections and Trojan infection attempts, involving 3 network-propagating malware samples.

A total of 103.2 hours of sustained, automated attacks were performed, in addition to extensive manual test design, set-up and analysis.

Individual TCP/IP based flags including, SYN, ACK, FIN and TCP in specific probing and manipulation operations were utilized.

The following data in tabulated and graphical format highlight the overall test results:

MCU 4200 Series

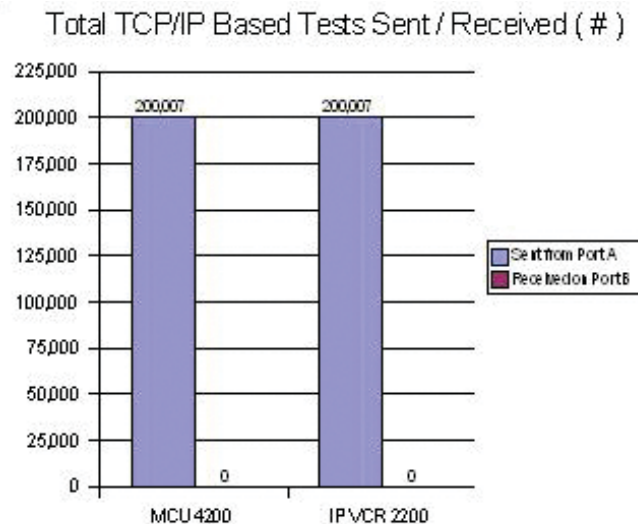
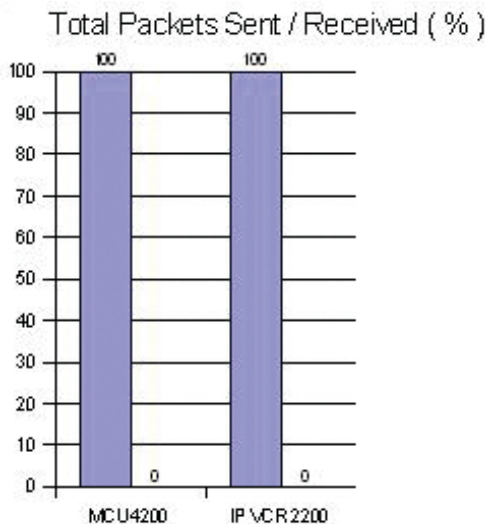
Total Packets (%)	
Sent from Port A	Received on Port B
100	0

Total TCP/IP Based Tests (#)	
Sent from Port A	Received on Port B
200,007	0

IP VCR 2200 Series

Total Packets (%)	
Sent from Port A	Received on Port B
100	0

Total TCP/IP Based Tests (#)	
Sent from Port A	Received on Port B
200,007	0



CONCLUSION



With zero packets transferred between the external and internal interfaces of each DUT throughout the test period, potential Codian customers can be confident in the security claims and capabilities of each device tested.

In relation to overall usability, each DUT proved easy to configure and administer using the web based management console, accessible via a standard web browser. The user interface was clean and well designed, ensuring that general administration tasks were simple to perform.

In the context of these specific tests, each product proved totally effective in dealing with an extensive range of targeted, real-world attacks.

ABOUT CODIAN

A decorative horizontal bar consisting of a blue segment on the left and a red segment on the right, positioned below the section header.

Codian designs and manufactures the most advanced video conferencing infrastructure products available. Codian's product line includes Multipoint Control Units, Video Conference Recorders, Streaming Servers and ISDN Video Gateways. Using a unique architecture and the latest hardware technology, Codian's products are both easy to use and powerful, supporting enterprise and service provider customers worldwide. Codian has main offices in San Jose, California; London, UK; and Hong Kong.

For a product demonstration or to learn more about Codian products, please visit the website at: www.codian.com.

ABOUT WEST COAST LABS

WCL is an independent technical consultancy, specialising in the independent testing and validation of the functionality and performance of information security products and services.

With a global client base of over 90 vendors, including the world's leading security technology developers, WCL has a reputation for technical expertise, quality of service and independence.

www.westcoastlabs.org



West Coast Labs, William Knox House, Britannic Way, Llandarcy,
Swansea, SA10 6EL, UK. Tel : +44 1792 324000, Fax : +44 1792 324001.
www.westcoastlabs.org

WEST COAST LABS STANDARD DISCLAIMER

While West Coast Labs is dedicated to ensuring the highest standard of security product testing in the industry, it is not always possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and / or functionality of any particular product tested and / or guarantee that any particular product tested is fit for any given purpose .

Therefore, the test results published within any given report should not be taken and accepted in isolation. Potential customers interested in deploying any particular product tested by West Coast Labs are recommended to seek further confirmation that the said product will meet their individual requirements, technical infrastructure and specific security considerations.

All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability. West Coast Labs provide test results for any particular product tested, most relevant at the time of testing and within the specified scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools used during the specific test process.

West Coast Labs is unable to directly endorse or certify the overall worthiness and reliability of any particular product tested for any given situation or deployment.

