newline CAST

Security Whitepaper

Tuesday, August 10, 2021

Index

Background

Newline Cast is a wireless presentation solution designed to allow users to stream video and audio from their devices to a Newline display.

Network configuration

Due to typical network set-up in an organisation, it is common to have guests and external users connect to a separate network than your internal users. This means there will be two different networks in your environment: an internal and a guest network.

DisplayNote supports such a configuration. Users can be connected to two networks simultaneously, enabling guests to connect and present while maintaining network security.

No action is needed for cross-network connectivity.

Network infrastructure

All inbound and outbound data from our backend layer is encrypted and transmitted over TLS or DTLS, with 2048-bit asymmetric encryption and 256-bit symmetric encryption using certificates from third-party credited authorities.

Network communication is protected using the latest in technology to secure all video, audio, and data. Using the TLS and DTLS cryptography protocols, previously referred to as SSL, we provide protection using a 2048-bit asymmetric key in conjunction with a 256-bit symmetric session key. More information on network ports used can be found further within this document.

The backend tier provides four public services:

- REST API
- XMPP and
- STUN / TURN

Newline Cast uses a combination of Azure and Amazon services to provide a resilient and redundant backend while delivering the lowest latency possible.

Azure

Azure's data centers are geographically dispersed and comply with ISO/IEC 27001:2005, SOC 1, and SOC 2 and have a CSA STAR certification.

These data centers are managed and operated by Microsoft. Microsoft has decades of experience building enterprise software and running some of the world's most extensive online services.

Using Azure's Network Security Groups (NSG), access to virtual machines hosting our services is limited to those ports configured within the NSG only.

All our virtual machines are located within the same virtual LAN, and communication between virtual machines is via private network interfaces behind the Azure firewall.

Amazon AWS

We also use Amazon AWS to host and support the services we offer to our clients. Amazon AWS is a well-known cloud service managed by Amazon, a trusted provider of cloud services that provide geographical dispersion - allowing us to have a server closer to the end-user, which reduces latency in cloud connectivity.

All our cloud services running on Amazon AWS are running under a Virtual Private Cloud (VPC). Each environment has its own virtual network protected by Amazon's availability zone and firewall.

Amazon AWS servers are geographically dispersed and have many certifications and third-party assessments, including ISO/IEC 27001:2005, SOC 1 and SOC 2, and CSA STAR certification. Further information can be found in their security whitepaper.

Network features

The Newline Cast software consumes a REST API provided by our SaaS layer, which is credential secured. All communication with the REST API and our XMPP services are over TLS (port 443) with 2048-bit asymmetric encryption and 256-bit symmetric encryption. For video calls, STUN is used to establish a peer-to-peer connection. If this fails, the client will attempt to use our relay service using the TURN protocol.

In addition to DTLS encryption, we also encrypt data through Secure Real-Time Protocol, which safeguards IP communications from hackers. This ensures your video and audio data are kept private point-to-point.

Cloud connectivity and local - only sessions

If Newline Cast has access to the cloud, it can allow devices to connect from outside of its local network. For example, a Chromebook client on a remote network and a Windows client connected on another network within your organization.

This can be restricted by deactivating access to the cloud in Newline Cast settings.

In local-only mode, users can only connect if they are on the same network.

Meeting ID and PIN

For each meeting, a unique meeting 6-digit session ID is generated. This is mediated from our SaaS layer, which is used for clients to connect to that specific meeting. If there is an internet connection, this meeting ID will be 6-digits long.

If no internet is available (or local connections only), the Meeting ID will be 10-digits long. This 10-digit meeting ID is generated using the device IP address, enabling connection from different subnets on the same network.

If devices connect using the 6-digit meeting ID, a connection is attempted locally. If this is not possible, the connection is made via XMPP. The host can also specify a PIN, configured at the box directly, and on each client connecting would request confirmation of the PIN.

Software updates

The Newline Cast receiver and DisplayNote enabled client app checks for software updates regularly. If there is an update available, users will get a notification when they open up the app. Click Update, and the application will install the latest update.

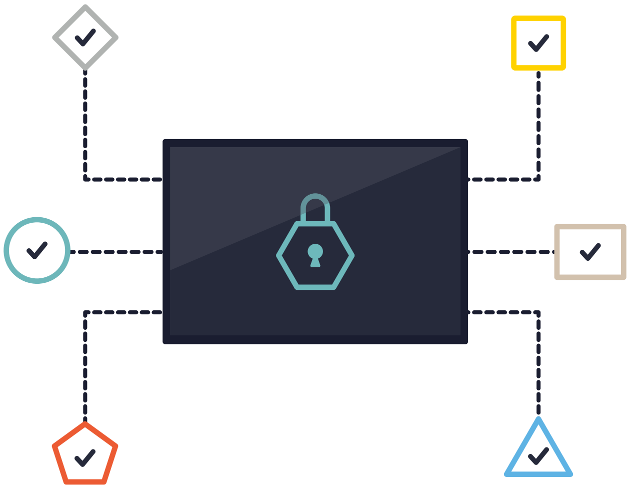
You can also download and install the latest version from our website, which will replace your previous version.

Mobile and web versions update automatically with no need to install or run updates. MSI versions of the app will need to be updated manually.

An internet connection is required for updates. The updates are downloaded over a secure connection (using port 443) and are installed on demand. A notification will appear in the Newline Cast user interface to indicate an available update that the user can install.

The clients and boxes are authenticated on our servers using a 4-step authentication process with SASL. At any time, administrators can remove a client or box from the authorized zone temporarily or permanently.

All data transferred between the user's device and Newline Cast is peer-to-peer (P2P) and is over TLS or DTLS with 2048-bit asymmetric encryption and 256-bit symmetric encryption. If a P2P connection fails to connect between the client and Newline Cast , the software will relay the data via our TURN server over TLS TCP port 443.



Firewall s and proxy

Firewall s

For remote connections, both receiver and clients need to be able to access the internet through these ports:

- TCP 80
- TCP 443
- UDP 53

For local connections, i.e. Clients on the same network) the following ports are used:

- TCP 1-65535 (It will be selected from available ones)
- UDP 1025 – 65535
- TCP 4700, 7000, 7100 (For Airplay connections)
- TCP 8009 (For GoogleCast services)

If there is Layer 7 filtering or proxy with protocol filtering on these ports, then the following protocols will need to be allowed:

- HTTP
- HTTPS
- DTLS
- XMPP

- Bonjour protocols
- SRTP
- DNS
- STUN
- TURN
- ICE

Our SaaS provides services at the following FQDNs;

- Newline Cast.displaynote.com
- xmpp.displaynote.com
- stunturn-prod-ireland.displaynote.com
- stunturn-prod-mumbai.displaynote.com
- stunturn-prod-singapore.displaynote.com
- stunturn-prod-virginia.displaynote.com
- stunturn-prod-california.displaynote.com

Proxy support

The Newline Cast Windows/OSX software support proxy configuration. The following proxy types are supported.

- HTTP Proxy (with or without authentication)
- SOCKS 5 (with or without authentication)
- Proxy with Auto-Configuration File (PAC). Windows only.
- System proxy. Windows only.

Security

The clients and receivers are authenticated on our servers using a 4-step authentication process with SASL. At any time, administrators can remove a client or receiver from the authorized zone temporarily and permanently.

All data transferred between the user's device and Newline Cast is peer-to-peer (P2P) and is over TLS or DTLS with 2048-bit asymmetric encryption and 256-bit symmetric encryption. If a P2P connection fails to connect between the client and Newline Cast , the software will relay the data via our TURN server over TLS TCP port 443.

Penetration Testing

Executive Summary

Nexusguard Consulting Limited (hereinafter "NCL", "us") was assigned by DisplayNote Technologies to facilitate "Penetration Testing & Application Testing" on its applications (hereafter "**Project**") in 28 Oct 2020. The goal of this project mainly focuses on below objective(s):

- Identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components.
- Verify that only authorized services are exposed at client network
- Attempt to bypass authentication controls from all network segments where authorized users access the internal resources, as well as segments not authorized to access internal resources

- Develop a final report with all identified system, network, and organizational vulnerabilities and provide recommended mitigation actions

This project was conducted alongside a DisplayNote end user and is therefore intended to provide the security assurance on defending both application level and network level attack with a DisplayNote customer's backend. While the findings below are intended to broadly demonstrate DisplayNote's security credentials, it was carried out with a specific customer and therefore findings are specific to that's customer's backend.

Result Summary

The results summary that NCL has discovered during penetration testing:

- NO risks have been found

During the external penetration testing process, NCL has not discovered any vulnerabilities or exploitable entry points.

Testing Methodology

NCL Penetration Testing Methodology was developed based on NIST SP800-115 Technical Guide to Information Security Testing and Assessment and PCIDSS Penetration Testing Guidance version 1.5. Our Methodology is suitable for both black-box testing and white-box testing and helping to improve the effectiveness and efficiency of penetration testing. Our methodology contains four typical phases that occur during the whole penetration testing process to ensure the successful rate of our testing. Those phases including: Planning, Discovery and Identification, Execution and Post- Execution and Reporting.

Planning Phase

The main goal of this phase is gathering information needed before assessment execution. Thus, NCL invites all related parties to provide pre-engagement information and informs them which type(s) of testing would be performed. NCL collects necessary information from related person and defines the baseline of this testing such as scope, requirements, team roles and responsibilities, limitation , success criteria and all elements related to project management.

Discovery a nd Identification Phase

Primary goal of this phase is discovering and identifying which services and ports are targets running. NCL is able to analysis target services status, version and back-end information to find out possible exploitable point according to collected information. This phase also performs an aggressive vulnerability discovering to find out vulnerabilities that would not be discovered by passive vulnerability scanner.

Execution and Post -Execution Phase

This phase is verifying whether vulnerabilities are found in last phase and whether is exploitable. NCL tries to take any actions after the initial compromise of a system or device. The execution is focusing on application layer and network layer, verifying client configurations and attempt to bypass authentication controls. Once the exploitation is complete and success, NCL can perform the “post-execution” actions such as privilege escalation, gain additional access to system or network resources or create a new attack source. Baselines and limitations in this phase defined in planning phase and approved by both Client and NCL.

Reporting Phase

Upon completion of the testing, a report establishes and includes all the actions taken during the testing, evidences, and exploitable and non-exploitable vulnerabilities, findings and recommended mitigation actions. Also, the result of report is able to meet reporting requirements of compliance and should present by NCL team.

Result s

Findings

NCL has discovered two low risk vulnerabilities or exploitable entry points of DisplayNote's customer. It proves that all configurations and implementations of customer scope have fulfilled security best practices.

Recommendations

The result of this Penetration Testing and application test reflect that the scope has fulfilled security best practices. However, as a professional information security company, NCL recommends following actions to improve their performance and efficiency after penetration testing:

- Regular scanning shall be performed for backend servers since security patches and vulnerabilities are updating every day. To keep server up to date on security level, penetration testing once per year is also required.
- System hardening and configuration review on related machines is the best practice on protecting backend server and data stored in server.

Pre-Engagement

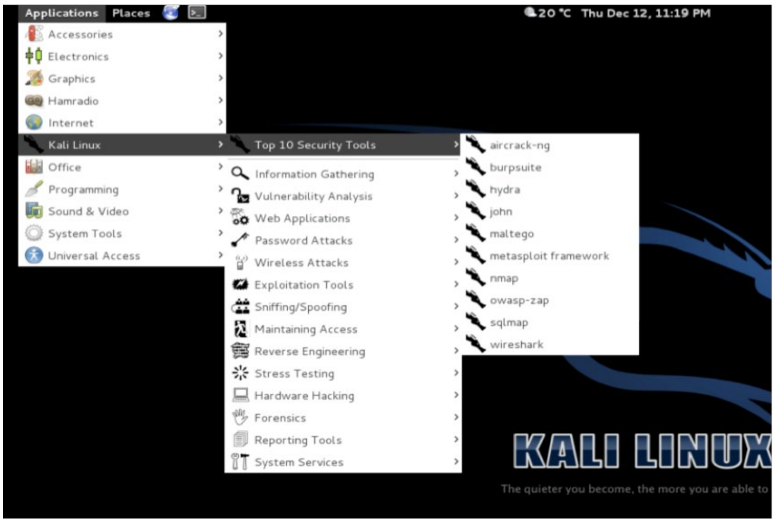
Blackguard Information

Type of Testing	External White-box testing	
Date	28-OCT-2020	
Time	1630 - 2000	
Scoping		
Hostname	IP Address	Host Nature
dn-broadcast.displaynote.com	178.128.200.49	Web Server
broadcast-license.displaynote.com	23.100.9.226	Web Server
broadcast-license.displaynote.com/broadcast/api	23.100.9.226	API Server
montage.displaynote.com/montage/rest	23.100.9.226	API Server
xmpp-prod-1.cloudapp.net	23.101.75.146	XMPP Server
heavy-duck.rmq.cloudamqp.com	54.72.85.144	CloudAMQP Messaging
displaynoteshadow.azurewebsites.net/api	104.45.14.249	API Server
launcher-service.azurewebsites.net/api	40.114.210.78	Web Server
Vulnerability Level Definition		
Source Name	Reference Link	
Common Vulnerability Scoring System Version 2 Calculator	http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2	
Penetration Testing Team Member		
Name	Email	
Eric Yeung	Eric.yeung@nexusguard.com	
Andy Lam	Andy.lam@nexusguard.com	

Pre-Engagement Preparations

Testing Environment **Kali Linux**

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. Kali Linux is preinstalled with numerous penetration-testing programs, including nmap, Wireshark, John the Ripper, Scapy , Hping3 , Openvas , Wa3f ,ettercap , Xplico , netcat . It is a supported platform of the Metasploit Project's Metasploit Framework, a tool for developing and executing security exploits.



Vulnerabilities Identification and Analysis

NO Vulnerability has identified during external PCI penetration testing.

Execution and Post - Execution

Execution Details

NCL has not conduct ANY execution activities because no vulnerability has discovered.

Post - Execution

NCL has not conduct ANY post-execution activities because all of execution findings are not required those tests to prove its existence.

Technical Detail

OWASP Top 10

Item#	Name	Pass / Fail
1	Injection	Pass
2	Broken Authentication	Pass
3	Sensitive Data Exposure	Pass
4	XML External Entities (XXE)	Pass
5	Broken Access control.	Pass
6	Security misconfigurations.	Pass
7	Cross Site Scripting (XSS)	Pass
8	Insecure Deserialization	Pass
9	Using Components with known vulnerabilities	Pass
10	Insufficient logging and monitoring	Pass

Injection

Our Penetration testing team has discovered web services / API service that is running 443. We have tried different injection methods to do so. Example Payload as below:

- ?id=' or '1'='1
- <script>alert("XSS Testing");</script>

As all servers are escaping special characters and hence no injections are successfully injected.

Broken Authentication

All Authentications are protected by TLS 1.2, in current technologies, it takes a very long time in terms of years

Sensitive Data Exposure

As stated above, all data has been encrypted during the transmission and no sensitive information is being disclosed. Moreover, no other components are disclosed in packet levels, code levels and application level.

XML External Entities (XXE)

This Vulnerability is referring to XML configurations and document disclosure in advance. During the penetration test, we do not find any XML that can be called in API servers.

Broken Access control

As API servers do not have a page for login purpose and no findings here.

Security misconfigurations

As our project does perform vulnerability scanning and no misconfigurations were found

Cross Site Scripting (XSS) Same as 1.

Insecure Deserialization

It is about data passing and modified when Man-in-the-middle setup, no issues were found.

Using Components with known vulnerabilities

No components were discovered that is well known in high vulnerability

Insufficient logging and monitoring

The system is on cloud and whitelisting practice is in place and hence newline

HEAD OFFICE
EMEA
Ronda de Poniente, 16,
Bajo E-28760, Tres
Cantos, Madrid, Spain
TEL: +34 911169178

BRANCH OFFICE
POLAND
Aleje Jerozolimskie 200,
pokój 322, 02-486,
Warszawa, Poland
TEL: +48 533379973

BRANCH OFFICE
GERMANY
Am Münster 36,
37154 Northeim,
Germany
TEL: +49 55515889580

SHOWROOM/OFFICE
ITALY
Via Giuseppe Giusti 10,
20068 Peschiera
Borromeo – MI, Italy
TEL: +39 3351295904

www.newline-interactive.com