BETA

SIMULATION SOLUTIONS

physics on screen

neere

ENOUGH
WITH DISTANCE

Questions & Answers on Data & Systems Security

Document version: 1.0 - August 2020

Summary

NEERE is an on-premises, web-based remote-working and collaboration environment, developed and distributed by BETA CAE Systems. NEERE bears all the security features to ensure the safety and confidentiality of communication.

BETA has deployed a NEERE instance on its own server to offer customer services such as, technical support and training. The data security policies of BETA, along with the NEERE features, ensure the data security and confidentiality of any web-session on this NEERE instance.

Partners and IT specialists are invited to adopt NEERE as a trusted application within their environment.

Introduction

NEERE is an on-premises, web-based tele-collaboration environment, tailor-made for the engineering community. Combined with ANSA, META, and META VR, NEERE provides a complete communication hub that makes sharing of knowledge and exchange of ideas effortless.

Work-from-Home becomes efficient and teams of interdisciplinary members can now work together in real-time technical meetings, fostering innovation and reducing virtual product development cycles.

NEERE enables remote work and teamwork, and boosts productivity through the direct engagement of users from all over the globe, in a secure, enterprise-ready, multi-OS web-platform.

This document aims to provide details and answer questions regarding NEERE security.

BETA CAE Systems software security

At BETA, security is always a top priority when designing and developing our products and NEERE does not fall out of that rule.

When a question of security arises, we always choose security over cost. To make sure that our partners are confident that their data is safe when using NEERE in their daily routine, we have deployed:

- Our very own coding guidelines.
- Automated penetration tests on each process separately.
- Automated penetration tests on NEERE as a whole.
- Dedicated QA team.

NEERE security

NEERE is an on-premises platform. This means that the NEERE server has the same security level as the actual server/network where it is installed.

On an application level NEERE is secured on multiple levels:

- Authorization on every action.
- Machine-to-machine encryption.
- Confidential data download restriction.
- Different level of user access.

Penetration Test and Vulnerability Assessment

BETA CAE Systems engaged NCC Group to perform a web application penetration test to assess whether NEERE is secure in handling sensitive data, as well as to ensure it neither allows unauthorised access nor contains other security related issues.

NCC declares that the NEERE web application was overall well designed with no high risk or critical findings. Any lower risk issues uncovered during the assessment can be mitigated as part of a defense-in-depth approach; nevertheless, it is reported that they are highly unlikely to pose a threat in a realistic scenario.

The backend VNC server was found adequately hardened with sufficient file permissions, which do not allow for privilege escalation attacks. In combination with the tight network controls in place, the likelihood of a successful attack is considered very low.

The respective documentation by NCC Group can be made available, to authorized stakeholders, upon request.

Authentication/authorization

Users are stored securely along with their privileges and with their passwords hashed. It is also possible to federate identity management to existing infrastructure such as, LDAP or Active Directory or use external identity providers using OpenID Connect and SAML 2.0 protocols, in which case no user storage is needed.

Authentication uses a Single Sign-On (SSO) mechanism and can be configured from a simple username-password pair, to two factor authentication or client certificates.

Authorization utilizes OAuth 2.0 Protocol which is the industry standard protocol for authorization.

NEERE consists of multiple standalone processes. Each of these processes is responsible for performing certain tasks. Every action performed by any user and any process in NEERE must be authorized via a secure short lifespan access token (1 minute - configurable). This makes sure that users can only access allowed resources and that no session can be highjacked. An administrator can add or remove permissions from any user with changes made effective almost real-time.

Identity and access management is handled by Keycloak, a software aimed at securing modern applications, developed by Jboss, a division of RedHat. For further details, visit: https://www.keycloak.org/

Encryption

All interprocess network traffic is encrypted with TLSv1.2 or later and with AES256, AES128 and EECDH+aRSA+SHA384 cyphers.

Traffic between server and clients is also encrypted.

HTTP traffic is secured with TLSv1.2 and later using the certificate provided by the administrator during the installation as described above (TLSv1.2+ with AES256, AES128 and EECDH+aRSA+SHA384).

WebRTC traffic (used for Audio/Video communication and View-Only screen sharing) is encrypted with DTLS 1.0 when UDP is used, TLSv1.2+ when TCP is used.

Outgoing VNC traffic (used for Remote-Control screen sharing) is tunneled through an SSL socket.

Signaling and Incoming VNC traffic is tunneled through secured websocket (WSS using the same encryption as HTTPS traffic).

Additionally, when NEERE is installed on a private network, all data are transferred via the company's own network only.

Confidential data

NEERE enables collaboration of BETA CAE applications in a simple and intuitive way. However, launching ANSA and META via a web-browser, without the need of a local installation of these applications, may raise security concerns: “will confidential models be accessible to anyone?”, “can confidential data be downloaded locally?”, “can anybody delete an important file from the server?”, “will the data per se be streamed over the network?”. The simple answer to all these questions is: “no”.

NEERE allows mapping of NEERE users to system users for the execution of remote applications. This means, that each and every NEERE user can have different privileges on the filesystem exactly as configured by the system administrator for the user mounting the drive. So the filesystem ownership and permission are applied to NEERE users.

In Remote applications scenario all data stay on the server and cannot be downloaded.

The only traffic streamed from the server to the client is the image data from the virtual desktop in which the Remote Application is running. This traffic is of course encrypted with TLS.

In Local applications collaboration, the actual file data are not transmitted. The only traffic between CAE applications are the commands, so all ends of the collaboration scenario must have access to the same file in order to collaborate. Of course, the commands streamed are encrypted with TLS.

User passwords are hashed and not accessible by anybody. Deleted users are deleted irrevocably, while guest user data become anonymized upon invitation’s expiry.

User roles

There are two different user types in NEERE:

- Standard: can create rooms, can start remote applications, can view contacts.
- Guest: cannot create rooms, cannot start remote applications, cannot view contacts.

The main idea is that standard users are certified and trusted by the company, so they can manipulate server resources and invite guest users.

Guest users can still launch local applications and use NEERE for video/audio/text conversations if their invitation to a room is still active.

Only the system administrator has access to the user management console.

Additionally, in every remote application or remote desktop scenario, the owner of the application (the standard user who started it) determines who can operate the application and who can just view without operating. If the owner leaves the session (e.g. their network failed), then all other users are converted to viewers and they cannot operate the application any more.

NEERE for BETA's services

BETA deployed a NEERE instance on the public internet at https://neere-public.beta-cae.com. This NEERE instance, as a service, is intended to be used between BETA employees and partner companies as a means of secure communication for services such as meetings, remote training sessions, webinars and technical support.

A partner user must be invited by a BETA CAE Systems employee to have access to a service session. The only data required is a valid email address from the partner's corporate email domain.

The service is hosted in a server at the BETA CAE Systems HQ Datacenter, and is protected by the corporate firewall.

Physical access to the server is allowed only to authorized, properly identified and certified IT staff, while terminal and superuser access is only allowed from within BETA CAE Systems internal network.

Conclusion

NEERE covers many remote working and collaboration scenarios without sacrificing security for ease-of-use.

In BETA CAE Systems we continuously strive to deliver a stable, secure and hassle-free product using only well-established, state-of-the-art techniques.

Partners and IT specialists are invited to adopt NEERE as a trusted application within their environment.

For further questions, contact: ansa@beta-cae.com.

BETA CAE Systems International AG
D4 Business Village Luzern, Platz 4
CH-6039 Root D4, Switzerland
T +41 41 545 3650, F +41 41 545 3651
ansa@beta-cae.com
www.beta-cae.com

physics on screen