This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Genesys Security Deployment Guide

Open Web Application Security Project

5/4/2025

Open Web Application Security Project

Contents

Open Web Application Security Project (OWASP) is a world-wide organization that drives the evolution of safe and secure software, and the visibility and awareness of the need for it. It does not provide security solutions. Instead, it identifies and brings security issues to the attention of the software industry encouraging the industry to addressing these issues in their software.

OWASP is perhaps best known for its Top Ten Application Security Risks, commonly referred to as the OWASP Top Ten. This is a list of what OWASP considers to be the ten most important web application security weaknesses, and provides information to help address and mitigate these weaknesses. The weaknesses identified by the OWASP Top Ten have and will change over time, as software and the digital infrastructure becomes more complex and open. For more information about OWASP, the OWASP Top Ten, and what companies and organizations are using OWASP Top Ten, refer to the OWASP website.

This section identifies what and how Genesys addresses the OWASP Top Ten Weaknesses.

Top 10 2010-A3—Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.

To mitigate the risk of improper access to session-related data stored in cookies, Genesys uses the HTTPOnly and Secure flags when dealing with cookies related to web application sessions. The HTTPOnly flag prevents access to the cookie from non-HTTP protocols; the Secure flag prevents access outside of an SSL session.

Supporting Components

The following components address OWASP Top 10 2010-A3:

- Genesys Administrator
- Genesys Administrator Extension

Top 10 2007-A6—Information Leakage and Improper Error Handling

Error messages generated by failed authentication attempts used to display specific information about why the attempt failed. This could be used by an unauthorized user to gain access to the Genesys system. For example, one error used to indicate that either the login username or the password was incorrect. A malicious user could use this information to discover credentials, and gain access to data.

Now, the information returned by failed authentication requests, while still clear about the nature of

the error, is less specific about its cause. In the above example, the message still indicates that it is an authentication error, but combines the possible causes into being the username and/or the password. A malicious user would then have to try all possible combinations of all possible usernames and passwords, a task that is much greater than trying just a password or username.

Supporting Components

The following Genesys components address OWASP Top 10 2007-A6:

- Management Framework
- Genesys Administrator