GRAPECITY DOCUMENTS FOR EXCEL SECURITY

Standards and Policy

Abstract

This document describes the Security Assurance System, Standards, and Security Policy used for development and continuous integration testing of GrapeCity Documents for Excel. Through detailed and frequent security reviews, testing, and consulting based on OWASP TOP 10 security standards, we have developed security policies to ensure that GrapeCity Documents for Excel meets your code security needs, especially in relevant areas such as parsing, serialization, file input and output, and web access. These policies include using log security, data encryption, data protection, and controlling data availability to the end-user.

GrapeCity

Tel: 400-657-6008

Contents

Overview

The purpose of this white paper is to introduce the GrapeCity Documents for Excel (**GcExcel**) product security system and processes. The main contents include the following:

- Introducing the GcExcel Security Assurance System
- Introducing the security specifications and standards that GcExcel follows
- Introducing the GcExcel specific security policy

This white paper applies to the following user roles for reference.

- Software Developer
- Software Project Manager
- Software Security Specialist
- Security Requirements Staff

About GcExcel

GcExcel is a server-side high-performance component that creates, loads, edits, prints, and imports/exports **Microsoft Excel®** documents in bulk on the server-side, providing a complete Excel-like full-stack solution for user-developed applications and includes front- and back-end data synchronization, online filling, and server-side bulk export and printing of online documents for user-developed applications, as well as Excel-like report template design and server-side high performance processing, with no actual dependencies on **Microsoft Excel®**.

- **Component architecture is flexible and efficient: GcExcel** consumes far less memory and CPU time than enterprise project standards when processing Excel documents. **GcExcel** is much faster with enhanced performance and requires less memory consumption than POI.
- **Compatible with SpreadJS front and back ends: GcExcel** is naturally compatible with **GrapeCity SpreadJS** front and back ends and can directly import SSJSON format without dependency on Office or POI, providing an Excel-like full-stack solution for applications.

- **Excel-based document object model:** you can import, export, calculate, query, and generate Excel scripts.
- **Rich variety of themes and interfaces:** GcExcel provides many fully functional custom themes, component interfaces, configurable properties, data aggregation methods, embedded drawing objects, and a built-in calculation engine.
- **Highly compatible with Excel:** non-destructive import/export of Microsoft Excel® files, including pivot tables, tables, charts, comments, conditional formatting, data validation, formulas, shapes, images and mindmaps.
- **Accelerated cloud application development:** supports public cloud, private cloud deployment and standalone server deployment.

About GrapeCity

GrapeCity always adheres to the **High-End, High-Value** product concept, and works upstream in the IT industry chain to help and empower developers worldwide, providing secure and reliable technology products to help developers complete their business needs efficiently and with high quality.

Security Assurance System

The **GcExcel Security Assurance System** provides comprehensive security assurance for the software lifecycle, which extends through all phases of software requirements, design, development, testing and deployment.

Agile Development

GcExcel uses an agile development model in which project managers set iteration plans and milestones, and teams continuously follow up on issues and recheck them at critical points. At the same time, the development team ensures software security and quality through formal and informal code reviews. Revisits include and are not limited to the following forms:

- Stand-up sessions
- Daily code review meetings
- Agile Sprint Code Review Meeting

Continuous Integration

The **GcExcel** product is essentially a set of software toolkits whose products are built and exported by a continuous integration environment. In continuous integration, the following steps are included to improve the quality of security.

- Virus Scan
- Static code checking
- Automated test scripts

Among other things, virus scanning is used to review the product for the accidental inclusion of malicious programs. Static code inspection is used to scan source code for security issues and instantly track code security quality. Automated test scripts, on the other hand, ensure automated testing and regression testing of critical security modules and security issues by replacing human labor.

Architecture Review

When there are major feature updates to **GcExcel**, an internal architecture security review meeting is initiated by our team of security professionals, who discuss and examine the security requirements and response options for the product features.

Security Testing

GcExcel is thoroughly tested by our team of security professionals with professional testing methods and tools before each major version release to ensure product security. Security testing is built on the following security practice standards.

- **OWASP Top 10** (https://owasp.org/www-project-top-ten/)

Security testing is technically supported by in-house professional security reviewers and includes the following.

- Manual code review
- Static/dynamic code checking
- Third-party reliance on security checks

Security Consultation

GcExcel provides user-oriented security consulting services. When users ask questions related to product security, our in-house professional security specialists will respond positively and give an answer immediately after the investigation is completed. The consulting service covers the following.

- Pre-sales security consulting
- Provide product safety reports
- Interpreting third-party security review reports

Safety Training

At **GrapeCity**, we increase the safety awareness and competence of our employees by.

- New Employee Orientation Safety Training
- Freetalk security topic sharing
- Regular training on employee safety topics

Standards

GcExcel products are available to users worldwide and comply with the following common security standards set by international security organizations.

OWASP TOP 10 (2017)

The **OWASP Top 10** project (https://owasp.org/www-project-top-ten/) was originally aimed at raising security awareness among developers and managers, but it has become the actual Web application security standard. **OWASP Top 10** provides basic methods for preventing high-risk problems from occurring and provides guidelines for obtaining secure code. Since **GcExcel** is often integrated into Web applications as a component, the standards in this document apply.

- **Injection:** Injection flaws such as **SQL injection**, **NoSQL injection**, **OS injection**, and **LDAP Injection** can occur when untrusted data is sent to the parser as part of a command or query. Malicious data from an attacker can trick the parser into executing unintended commands or accessing data without proper authorization.
- **Authentication failure:** Often, by misusing the authentication and session management features of an application, an attacker can decipher passwords, keys, or session tokens, or exploit other development flaws to temporarily or permanently impersonate another user.
- **Sensitive data exposure:** Many Web applications and APIs fail to properly protect sensitive data, such as financial data, medical data, and **Personal Identifiable Information** (PII) data. Attackers can commit credit card fraud, identity theft or other crimes by stealing unencrypted data. Unencrypted sensitive data is vulnerable to compromise; therefore, it is necessary to encrypt sensitive data, which includes data in transit, stored data, and browser interaction data.
- **XML External Entities (XXE):** Many older or misconfigured XML processors evaluate external entity references in XML files. Attackers can use external entities to steal internal data and shared files using URI file processors, by listening to internal scan ports, executing remote code, and performing denial-of-service attacks.

- **Improper Access controls:** When proper access controls are not implemented for authenticated users, an attacker could use these flaws to access unauthorized functions or data, such as: accessing other users' accounts, viewing sensitive files, modifying other users' data, changing access rights, etc.
- **Security configuration errors:** Security configuration errors are the most common security problem, which is usually caused by insecure default configurations, incomplete temporary configurations, open-source cloud storage, incorrect HTTP header configurations, and detailed error messages containing sensitive information. Therefore, not only do we need to securely configure all operating systems, frameworks, libraries, and applications, but we must also patch and upgrade them in a timely manner.
- **Cross-site scripting (XSS):** XSS flaws occur when new pages of an application contain untrusted, improperly validated or escaped data, or when existing pages are updated by a malicious site using a browser API that can create HTML or JavaScript.
- **Insecure deserialization:** Insecure deserialization can lead to remote code execution. Even if deserialization flaws do not lead to remote code execution, attackers can use them to execute attacks, including replay attacks, injection attacks, and privilege escalation attacks.
- **Use components with known vulnerabilities:** Components (e.g., libraries, frameworks, and other software modules) have the same privileges as the application. If a component of an application with known vulnerabilities is exploited by an attacker, it can cause severe data loss or server takeover. Also, applications and APIs that use components with known vulnerabilities can compromise application defenses, cause a variety of attacks, and have serious implications.
- **Inadequate logging and monitoring:** Inadequate logging and monitoring, as well as missing or ineffective integration of incident responses, allow attackers to further attack systems, maintain continuity or move to additional systems, and tamper with, extract, or destroy data. Most defect studies show that defects are

not detected for more than 200 days and are typically detected through external detectors rather than through internal processes or monitoring.

Security Policy

Different security threats require different security mechanisms to prevent them, and the following introduces specific strategies for **GcExcel** to defend against security threats.

Serialization

Two technologies, XML serialization and JSON serialization, are used in **GcExcel**. In the application development process, both serialization technologies have deserialization security vulnerabilities. The following two deserialization vulnerabilities have been effectively circumvented and protected in **GcExcel**:

- XXE External entity attack
- JSON type deserialization

File IO

There is interaction with a variety of external files in **GcExcel**:

- **HTML injection:** When exporting HTML files, user data will be exported as part of the HTML content, and **GcExcel** will transcode all user data to effectively prevent XSS attacks from occurring.
- **CSV injection:** When there is a value starting with a specific character ('=') in CSV, the value will be automatically treated as a formula. **GcExcel** provides the corresponding option to disable automatic formula conversion when importing CSV.
- **Excel macros**: **GcExcel** reads Microsoft Excel® files without executing any Excel macros.

Web Access

GcExcel does not include web access associated with user input in 4.0.

Log Security

When **GcExcel** uses logging for debugging, only a fixed summary of debugging information is output, and no external data is recorded.

Data Encryption

GcExcel does not use any of its own encryption algorithms.

Data Protection

GcExcel provides complete **Microsoft Excel®** workbook and worksheet protection.

Data availability

Denial-of-service attacks achieve service unavailability by exhausting the resources of the target computer.

- Large-scale formula calculation: **GcExcel** formula engine has super high performance and significant memory savings.
- Regular expression attack: all untrusted regular expression patterns are escaped.

Summary

GrapeCity is committed to providing solutions you can trust, and we are committed to providing stable, reliable, and compliant document components such as GcExcel, to protect systems and data with measures ensuring the security of the products, data and components. At the same time, we continue to introduce innovative security technologies enhancing and improving the security capabilities of our products.