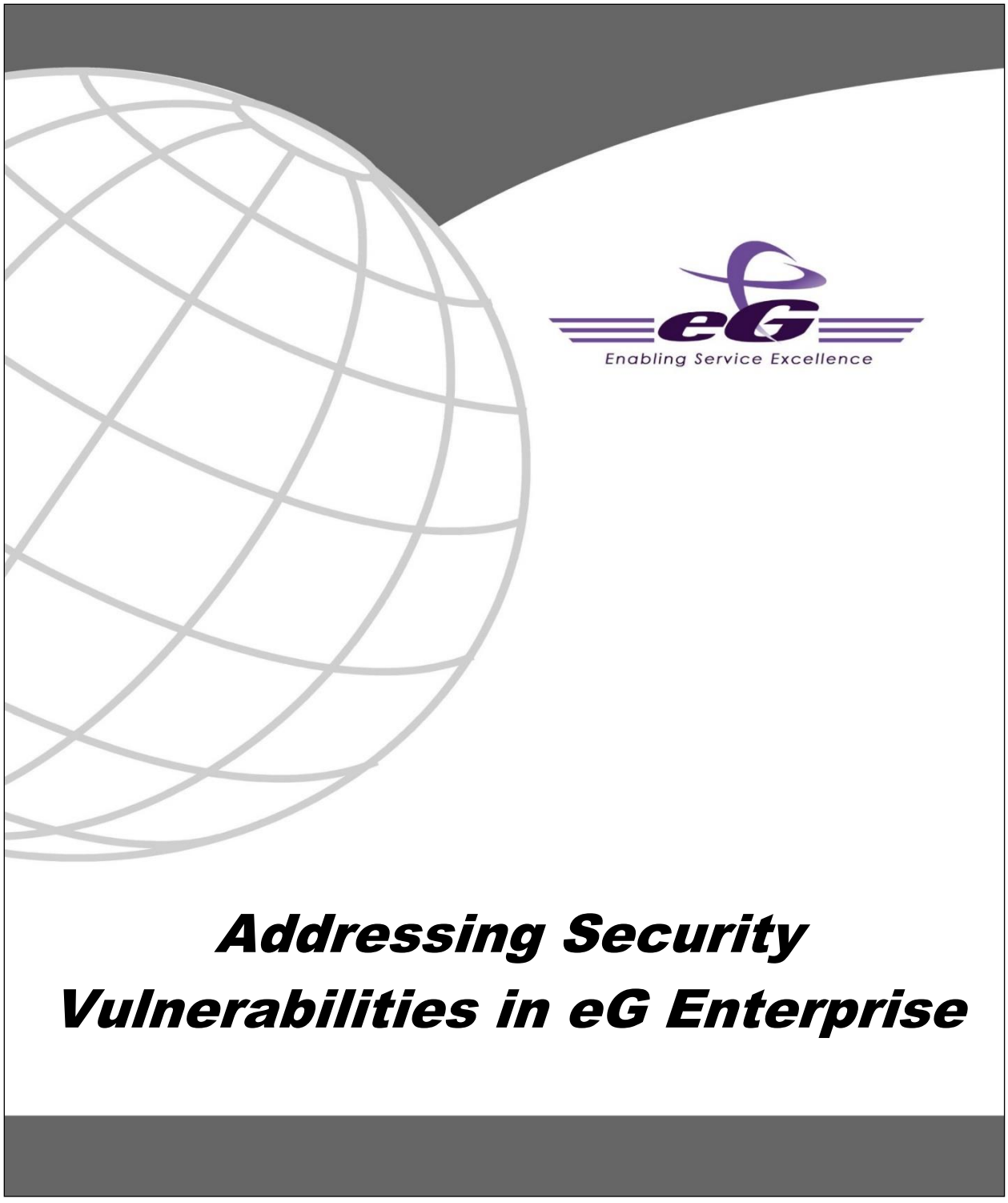

Addressing Security Vulnerabilities in eG Enterprise

Restricted Rights Legend

Trademarks

Copyright

Addressing Security Vulnerabilities in eG Enterprise

Recently, the following security vulnerabilities have been reported for the eG Enterprise manager:

- Improper access control and authentication: https://nvd.nist.gov/vuln/detail/CVE-2020-8591
- SQL injection vulnerability: https://nvd.nist.gov/vuln/detail/CVE-2020-8592

These vulnerabilities have since been fixed. The document discusses these vulnerabilities, enumerates the versions affected and how to fix them.

1.1 Improper Access Control and Authentication

This vulnerability allows a remote attacker to gain unauthorized access to otherwise restricted functionality of eG Enterprise. A remote attacker can bypass the implemented security restrictions via a "com.egurkha.EgLoginServlet?uname=admin&upass=&accessKey=eGm0n1t0r" request and unauthorized access to the eG Enterprise web console.

Versions Affected

Version 7.0, 7.1.0 and 7.1.2 of the eG Enterprise manager. Note that if you are using eG Enterprise version 6, this vulnerability does not affect your installation.

How to fix it?

Please contact your eG Innovations support team to get a consolidated patch to address this issue.

1.2 SQL Injection Vulnerability

The vulnerability allows a remote attacker to execute arbitrary SQL queries on the eG Enterprise database. The vulnerability exists due to insufficient sanitization of user-supplied data passed via the "user" parameter to "com.eg.LoginHelperServlet". A remote attacker can send a specially crafted request to the affected application and execute SQL commands on the application database.

Versions Affected

Version 6.3 and higher and Version 7, 7.1.0 and 7.1.2 of the eG Enterprise manager

How to fix it?

If you are using any of the versions listed under **Versions Affected**, then follow the steps below to fix this vulnerability:

1. Disable the **Forgot Password** link. For this, follow the steps below:
    - Login to the eG manager host.
    - Navigate to the <EG_MANAGER_INSTALL_DIR>\manager\tomcat\webapps\final\WEB-INF\classes\com\eg folder (on Windows; on Unix, this will be the /opt/egurkha/manager/tomcat/webapps/final/WEB-INF/classes/com/eg folder).
    - Search for the *LoginHelperServlet.class* file in the folder. Once it is found, rename the class file to say, *LoginHelperServlet1.class*.

- Restart the eG manager after making this change.

2. Turn on security filters. These security filters ensure that OWASP (Open Source Foundation for Application Security) recommended security best practices are implemented by the eG manager. Checks against SQL injection, Cross-site scripting (XSS), Cross-Site Request Forgery (CSRF) and other common types of attacks are implemented by these filters.

   To achieve this, follow the steps below:

   - Login to the eG admin interface.
   - Follow the Admin >>Settings>>Manager menu sequence.
   - Then, select the **Security Filters** sub-node from the **Account Security** node of the tree-structure in the left pane of the **MANAGER SETTINGS** page that appears.

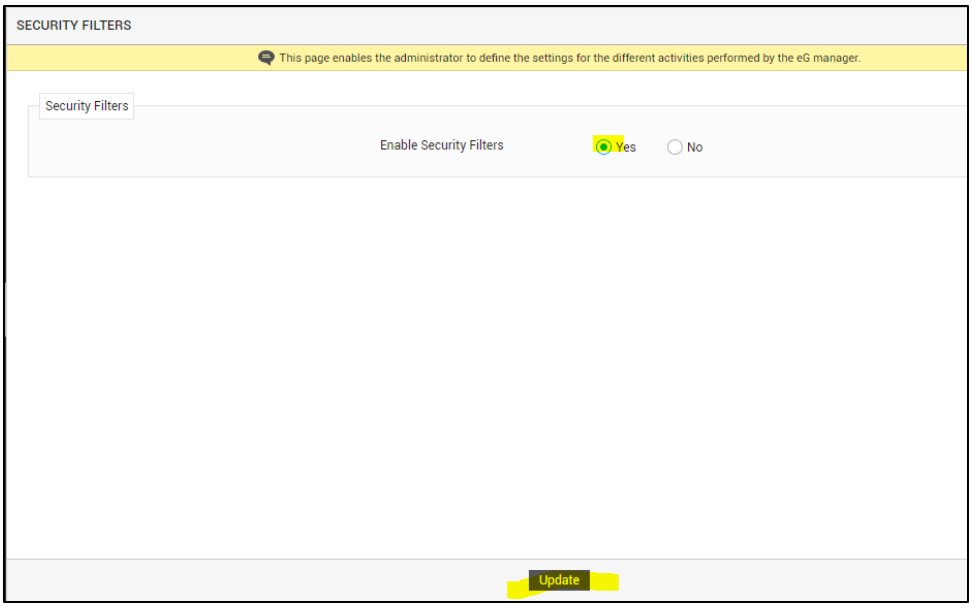

Figure 1: Enabling security filters

   - To enable security filters, set the **Enable Security Filters** flag in the right pane (see Figure 1) to **Yes**.
   - Then, click the **Update** button in Figure 2 to save the changes.
   - Restart the eG manager after making this change.

1.3 Other Recommended Security Precautions

- To ensure the security of the eG manager, ensure that you override the default passwords for the default accounts (admin and supermonitor).
- User accounts are hacked by repeated login attempts to the eG manager. To thwart such attacks, turn on user account security features in the eG Enterprise console. To enable these features:
  - Login to the eG admin interface.
  - Follow the Admin >>Settings>>Manager menu sequence.
  - Then, select the **Account Lockout** sub-node from the **Account Security** node of the tree-structure in the left pane of the **MANAGER SETTINGS** page that appears.

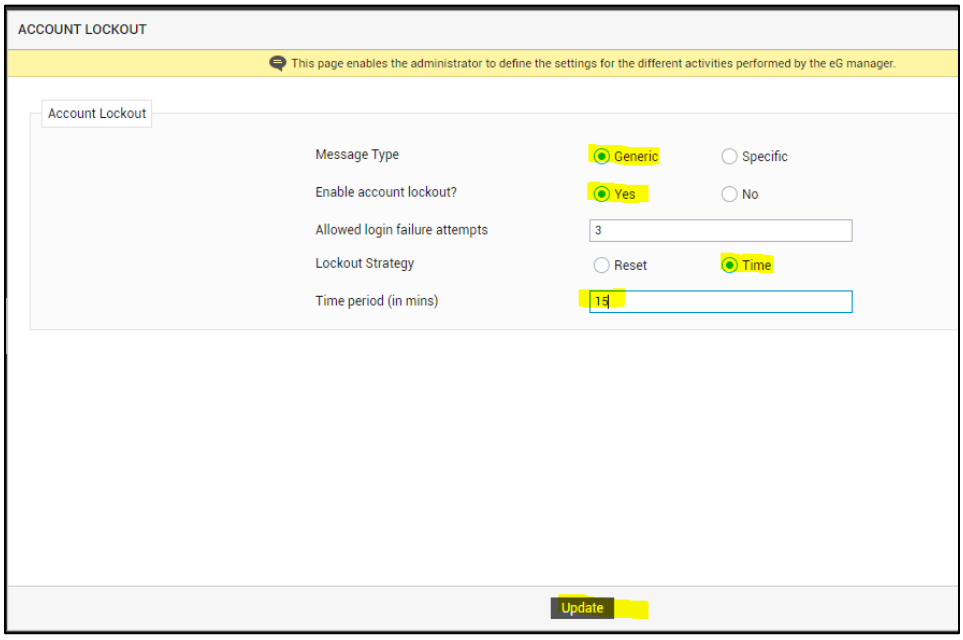

Figure 2: Enabling Account Lockout

- Using the **Account Lockout** section that appears in the right pane (see Figure 2), enable the **Account Lockout** capability of the eG manager. For that, first set the **Enable account lockout?** flag to **Yes**. Then, set **Message Type** to **Generic**, **Lockout Strategy** to **Time**, and **Time period** to **15** minutes.
- Finally, click the **Update** button in Figure 2 to save the changes.