OFFICE OF INSPECTIONS AND FORENSIC AUDITING
OFFICE OF INSPECTOR GENERAL
U.S. General Services Administration

MANAGEMENT ALERT REPORT:
GSA Data Breach

JE16-004
May 12, 2016

Summary

During the course of an ongoing evaluation, the OIG Office of Inspections and Forensic Auditing identified an issue that warrants immediate attention. Due to authorizations enabled by GSA 18F staff, over 100 GSA Google Drives were reportedly accessible by users both inside and outside of GSA during a five month period, potentially exposing sensitive content such as personally identifiable information and contractor proprietary information.

The purpose of this alert is to bring this matter to management's attention to ensure further vulnerabilities are appropriately mitigated and secured.

Findings

GSA employees in 18F are required by internal policy to use Slack, an online messaging and collaboration application, to share information such as files, images, PDFs, documents and spreadsheets. In order to permit the sharing of files from GSA Google Drive with team members in Slack, 18F uses OAuth 2.0, an authentication and authorization process. OAuth 2.0 can also be used to authorize access between the GSA IT environment and other applications as well.

On March 4, 2016, an 18F supervisor discovered that their use of OAuth 2.0 to authorize access between 18F's Slack account and GSA Google Drive permitted full access to over 100 GSA Google Drives, resulting in a data breach. On March 9, 2016, five days after discovering the breach, the 18F supervisor notified the GSA Senior Agency Information Security Officer of this vulnerability.

On May 5, 2016, during the course of an ongoing evaluation of 18F, the OIG became aware of the data breach and on May 6 questioned the supervisor about the incident. The supervisor told the OIG that although they became aware of the data breach in March, the vulnerability had been in existence since October 2015. The supervisor also advised the OIG that the full access OAuth 2.0 permissions between the GSA Google Drives and 18F's Slack account have since been eliminated.

18F's use of both OAuth 2.0 and Slack is not in compliance with GSA's Information Technology Standards Profile, GSA Order CIO P 2160.1E. The order allows information technologies to be approved for use in the GSA IT environment if they comply with GSA's security, legal, and accessibility requirements. Currently, neither OAuth 2.0 nor Slack are approved for use in the GSA IT standards profile.

In addition, by delaying the reporting of the data breach by five days, GSA 18F staff failed to comply with the GSA Information Breach Notification Policy, GSA Order CIO 9297.2B. The notification policy requires that all incidents involving a known or suspected breach of personally identifiable information must be reported to the GSA Office of the Chief Information Security Officer within one hour of discovering the incident.

The OIG makes the following recommendations:

1. GSA should cease using Slack and OAuth 2.0 until and unless they are approved for use in the IT Standards Profile.

2. GSA should ensure that 18F complies with GSA Order CIO P 2160.1E.

Please notify this office, within 10 days, of steps taken by GSA in response to this Management Alert. The Office of Inspections and Forensic Auditing will continue to evaluate the steps taken by 18F after identification of the incident.

OFFICE OF
INSPECTOR GENERAL
U.S. General Services Administration

For media inquiries
OIG_PublicAffairs@gsaig.gov
(202) 273-7320

REPORT FRAUD, WASTE, AND ABUSE!

(800) 424-5210

Anonymous Web Form

fraudnet@gsaig.gov

Want to be aware of information the instant it becomes publicly available?

SUBSCRIBE