

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

<https://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

08/24/2020

**SUBJECT:**

Multiple Vulnerabilities in IBM Security Guardium Insights Could Allow for Program Compromise

**OVERVIEW:**

Multiple vulnerabilities have been discovered in IBM Security Guardium Insights, the most severe of which could allow for the program to become compromised. IBM Security Guardium Insights is a program developed to monitor traffic traveling across the network to protect against data leakage and maintain data integrity. Successful exploitation of the most severe of these vulnerabilities could allow for a remote attacker to compromise the application. This could lead to data leakage or depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE:**

There are currently no reports of this vulnerability being exploited in the wild.

**SYSTEMS AFFECTED:**

- IBM Security Guardium Insights 2.0.1

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: N/A**

**TECHNICAL SUMMARY:**

Multiple Vulnerabilities have been discovered in IBM Security Guardium Insights, the most severe of which could allow for the program to become compromised. Details of these vulnerabilities are as follows:

- A clickjacking vulnerability exists that allows a remote attacker to hijack a victim's click actions. (CVE-2020-4165)

- An open redirect vulnerability exists that could allow a remote attacker to compromise the application. (CVE-2020-4598)

Successful exploitation of the most severe of these vulnerabilities could allow for a remote attacker to compromise the application. This could lead to data leakage or depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided from IBM to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services

#### **REFERENCES:**

##### **CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4165>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4598>

##### **IBM:**

<https://www.ibm.com/support/pages/node/6320069>

<https://www.ibm.com/support/pages/node/6320061>

#### **TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

<https://www.us-cert.gov/tlp/>