

Finding GTN-001: Hardcoded Credentials Stored in Registry Editor.

Severity: Critical

Vendor of the product: Isode, SWIFT

Product: SWIFT

Version: 4.0.2

Researcher: Pankaj Kumar Thakur (Green Tick Nepal Pvt. Ltd.)

**Product Link: <https://www.isode.com/products/swift.html>
<https://swift.im/downloads.html>**

Software Details:

Swift Desktop is a multi-platform XMPP client for instant messaging and multi-user chat. A free and open source client (with support packages available from Isode), it contains a number of features that make it ideal for use in secure environments such as Military, Finance and Government.

Finding Description:

I was taking snap shot of the registry before and after installation in order to see what changes were being made in the registry and I discovered hard-coded credentials and exposing (username, windows password, certificates, etc).

Impact:

Attacker might get all hardcoded Credentials from Registry Editor

Evidence:

Computer\HKEY_CURRENT_USER\Software\Swift\Swift

Computer\HKEY_CURRENT_USER\Software\Swift\Swift

Name	Type	Data
(Default)	REG_SZ	
lastLoginJID	REG_SZ	[REDACTED]@gtn.com.np
loginAutomatically	REG_SZ	true
[REDACTED]@gtn.com.np:certificate	REG_SZ	certstore:MY:sha1:ffeac978ccd925b9bffb6f8700f31d1b8408b4bd
[REDACTED]@gtn.com.np:jid	REG_SZ	[REDACTED]@gtn.com.np
[REDACTED]@gtn.com.np:options	REG_SZ	1,3,0,0,1,-,1,4,MTI3LjAuMC4x,1111,,,,0,
[REDACTED]@gtn.com.np:pass	REG_SZ	[REDACTED]
profileList	REG_MULTI_SZ	[REDACTED]@gtn.com.np

Suggested Remediation:

Remove Hardcoded Credentials from Registry editor.