Google works to close security loophole in Android

May 20 2011, By Nathan Olivarez-Giles

Google is in the process of updating its Android operating system to fix an issue that is believed to have left millions of smartphones and tablets vulnerable to personal data leaks.

"We recently started rolling out a fix which addresses a potential security flaw that could, under certain circumstances, allow a third party access to data available in calendar and contacts," a Google spokesman said in a statement. "This fix requires no action from users and will roll out globally over the next few days."

The fix is being issued for every version of Android released and began updating devices Wednesday, according to a person familiar with the software update who spoke on the condition of anonymity because of their relationship with Google.

The Mountain View, Calif., tech giant hasn't found any instances of hackers taking advantage of the flaw to steal a user's personal data, the person said, adding that Google hadn't known of the potential for such an exploitation until Germany's University of Ulm issued a report on the security hole.

"The implications of this vulnerability reach from disclosure to loss of personal information for the Calendar data," Ulm researchers Bastian Konings, Jens Nickels and Florian Schaub wrote in their report.

"For Contact information, private information of others is also affected,

potentially including phone numbers, home addresses and email addresses."

The vulnerability in Android was first pointed out by Rice University professor Dan Wallach in February, and the University of Ulm probed it further.

"Beyond the mere stealing of such information, an adversary could perform subtle changes without the user noticing," the Ulm researchers said. "For example, an adversary could change the stored email address of the victim's boss or business partners hoping to receive sensitive or confidential material pertaining to their business."

The flaw affected 99.7 percent of all Android smartphones and was not limited to Google Calendar and contacts, "but is theoretically feasible with all Google services," the University of Ulm said.

Among the weaknesses mentioned in the report was ClientLogin, which is Android's system to authenticate apps.

"Basically, to use ClientLogin, an application needs to request an authentication token (authToken) from the Google service by passing an account name and password via a https connection," the report said. "The returned authToken can be used for any subsequent request to the service API and is valid for a maximum duration of two weeks."

However, if the authToken is not encrypted and sent over an unsecured wireless network, "an adversary can easily sniff the authToken" and then use it to access any personal data which is made available to installed apps.

"For instance, the adversary can gain full access to the calendar, contacts information or private Web albums of the respective Google user," the

Ulm researchers said. "This means that the adversary can view, modify or delete any contacts, calendar events or private pictures. This is not limited to items currently being synced but affects all items of that user."

The tactic "is very similar to stealing session cookies of websites" or sidejacking, which is a popular attack among hackers breaking in to Facebook or Twitter accounts over unsecured wireless networks.