Security Advisory

MSL-2009-001
Samsung Missing Provisioning Authentication

Advisory Information

Title	Samsung Missing Provisioning Authentication
Advisory ID	MSL-2009-001
Advisory URL	http://www.mseclab.com/index.php?page_id=148
Published	2009-04-23
Updated	2009-04-23
Vendor	Samsung

Vulnerability Details

Class	Authentication Bypass
Remote	Yes
Local	No
Public References	Not Assigned
Affected	Samsung M8800 Innov8 Samsung SGH-J750
Not Affected	Unknown
Description	Affected devices do not perform proper authentication of incoming SMS Provisioning messages. The following behaviors have been verified on affected devices: 1.Source of provisioning message is never displayed to user. 2.Unauthenticated SMS Provisioning messages, where SEC and MAC parameters are not present in the message, are accepted. User is not made aware that the received provisioning message is not authenticated. 3.Authenticated SMS Provisioning messages, where SEC and MAC parameters are present in the message, are accepted, but the parameters are not used for performing the security checks. More specifically: •USERPIN authenticated provisioning message: device installs the received

	configuration without performing any message authentication. PIN Code is never asked to user and is not required for completing the installation. The installation is correctly performed and the configuration is installed as default. •NETWPIN authenticated provisioning messages: device installs the received configuration without performing any message authentication. Sender does not need to know the correct IMSI value in order to let the device accepts the message as correct. The configuration will be installed regardless of the MAC value present in the message. By sending provisioning messages in one of the above specified ways, an attacker could pose as a legitimate trusted source and entice a victim into installing a malicious configuration. Such an attack could lead to the hijacking of mobile data connections originated by the device.
Solutions & Workaround	Not available

Additional Information

Timeline	*2009-04-04:* Issue discovery *2009-04-06:* Initial Vendor Notification: Point of Contact requested via contact form on website (No suitable e-mail available) *2009-04-07:* Vendor Response: Automated response *2009-04-23:* Public Disclosure
Vendor Statement	None