Security Advisory

MSL-2008-001
SonyEricsson WAP Push Denial of Service

Advisory Information

Title	SonyEricsson WAP Push Denial of Service
Advisory ID	MSL-2008-001
Advisory URL	http://www.mseclab.com/index.php?page_id=123
Published	2009-01-26
Updated	2009-01-26
Vendor	SonyEricsson
Platforms	Multiple

Vulnerability Details

Class	Denial of Service
Remote	Yes
Local	No
Public References	Not Assigned
Affected	Multiple devices. Successfully tested on: •W910i •W660i •K618i •K610i •Z610i •K810i •K660i •W880i •K530i Other devices based on the same (or earlier) platform are likely to be vulnerable.
Not Affected	More recent devices may be not vulnerable.
Description	A malformed WAP Push packet is able to remotely reboot the handset and, in some cases, completely hang it.

	In case the handset hangs, battery removal is needed in order to restore normal functionalities. By sending multiple malformed packet via SMS, an attacker may be able to reboot the handset multiple times, effectively performing an extended denial of service. The attack can also be performed over an IP bearer using UDP port 2948. In this case a single malformed broadcast packet can be used to attack and disable a large number of devices, leading to a much heavier impact.
Solutions & Workaround	Not available

Additional Information

Vulnerability Status	The issue has been reported to SonyEricsson. Mobile Security Lab is aware that the problem has been identified: some models, more recent than the ones listed in this advisory, have been found not to be vulnerable. Further details are not currently available to Mobile Security Lab.
Vendor Statement	None