TD61-2716
HCVU000000004
Sep/30/2005
Hitachi Cable

WirelessIP5000: Multiple Vulnerability Notification

1. Summary

WirelessIP5000 has following multiple vulnerabilities.(JVN#76659792)

(a) Undocumented open port

Description: WirelessIP5000 Phone has a undocumented open port, TCP/3390, that may allow a remote unauthenticated attacker to access.

Impact: A remote unauthenticated attacker may be able to access sensitive information and potentially impact the phone's operations in a DoS.

(b) SNMP vulnerabilities

Description: A vulnerability exists in the WirelessIP5000 Phone that may allow a remote attacker to modify the configuration of the device using SNMP.

Impact: This vulnerability allows attackers to read and modify any SNMP object present on an affected device.

(c) HTTP authentication

Description: WirelessIP5000 Phone HTTP server default configuration does not require credentials to authenticate.

Impact: A remote attacker could perform administrative functions without authenticating.

(d) Sensitive information in HTTP

Description: There is a vulnerability in WirelessIP5000 Phone HTTP server that could disclose the sensitive information.

Impact: Sensitive information may be disclosed.

(e) Administrator password

Description: A default administrator password exists in WirelessIP5000 Phone. An attacker with knowledge of this information can compromise any of the devices.

Impact: An attacker with knowledge of default administrator password and the ability to access a vulnerable device may take administrative control of the device.

2. References

(1) JP Vendor Status Notes JVN#76659792 (Japanese)
http://jvn.jp/jp/JVN%2376659792

3. Software Versions and Fixes

Product	Version	Status
WirelessIP5000	1.5.0 1.5.2 1.5.4 1.5.5 1.5.6 1.5.8 1.5.10	Vulnerable, (a)(b)(c)(d)(e)
	2.0.0	Vulnerable, (a)(b)(e)
	2.0.1 2.0.3 2.1.0 2.1.2	Vulnerable, (e)

4. Solution

Upgrade to version 2.0.1 or later for these vulnerabilities.
And change an administrator password manually.

5. Acknowledgement

Thanks to Shawn Merdinger for reporting these vulnerabilities.