Security Advisory Report - OBSO-1010-01

Enabled VxWorks debug service

Creation Date: 2010-10-15
Last Update: 2010-10-15

Summary

A security researcher has identified a large number of products based on the VxWorks platform provided by Wind River Systems with a debug service enabled by default at port 17185/udp.

Vulnerability Details

The debug service provides full access to the memory of an affected device and allows for memory to be written as well as functions to be called.

Of the various products based on VxWorks, the following are not affected by this vulnerability: HiPath Wireless Convergence, RG 8700, optiPoint 410/420 SIP and HFA (V5).

Affected Products

- HiPath 3000 (HG 1500 Gateway)
- HiPath 4000 (HG 35xx Gateway)
- optiPoint 410/420 HFA, versions before V5
- optiPoint 600 office

Recommended Actions

In general, it is recommended not to attach the mentioned systems directly at the internet. Appropriate firewall rules should be implemented to restrict access to the debug service (17185/udp).

The problem is solved in the following versions; an update to these or higher versions is highly recommended:

- HiPath 3000 V8: V8 R5.2.0
- HiPath 4000 V4: V4 R4.1.12
- HiPath 4000 V5: V5 R1.2.4

Please note:

- HiPath 3000 V7: You need to upgrade the HG 1500 gateway only. Please use V8 R5.2.0 for this. You may keep the system itself in V7.
- HiPath 3000 V6 and earlier have reached end of SW support; please consider an upgrade to V7 or V8
- HiPath 4000 V3 and earlier have reached end of SW support; please consider an upgrade to V4 or higher.
- Some older, unsupported versions of optiPoint 410/420 HFA IP phones are also vulnerable. Please ensure, that V5 is installed on all phones.
- optiPoint 600 office has reached end of life since a few years already; an update is unfortunately not available

References

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2965
- http://blog.metasploit.com/2010/08/vxworks-vulnerabilities.html
- http://www.kb.cert.org/vuls/id/362332

Revision History

2010-10-15 Initial release

Contact and Disclaimer

OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.