UNIFY

Security Advisory Report - OBSO-1106-01

Allied Telesis divulges secret backdoor

Creation Date: 2011-06-07
Last Update: 2013-11-08

Summary

Allied Telesis accidentally put information about "backdoors" present in some of its products into the public support area on its web site.

Vulnerability Details

On May 27th 2011 information was published that Allied Telesis had accidentally put an internal document into the public support area on its web site. The document talks about "backdoors" present in some of its products and how to use them to reset the device's root access.

For more information of what information was leaked, refer to the example article by H-online (see link in the references section).

Affected Products

No products of Unify are affected.
Unify's Remote Service for access to HiPath 4000 solutions uses Allied Telesis routers of type AT-AR415S. According to the vendor's statement, these routers are not affected.

Recommended Actions

As per Customer Support Memo, June 1, Allied Telesis confirmed that this was an unintentional temporary disclosure of an internal document. However, having access to the information in this document does not enable anyone to log into any devices. No specific action is required.

In case of interest, ask your Unify contact, who can provide you with the detailed Customer Support Memo.

Furthermore, all AlliedTelesis routers which Unify delivers to their customers as part of the remote service solution, are not affected at all by the disclosed information.

References

- www.h-online.com/security/news/item/Allied-Telesis-divulges-secret-backdoor-1251556.html

Revision History

2011-06-07: Initial release
2013-11-08: Rereleased under the Unify brand (formerly Siemens Enterprise Communications)