Security Advisory Report - OBSO-1407-02

HiPath 4000 V6 - Security Updates for the Gateway Web Interface

Creation Date: 2014-07-23
Last Update: 2014-07-23

Summary

Unify has released an update for HiPath 4000 V6 R2 and the associated Security Checklist to

- resolve multiple vulnerabilities in the administration web interface on HiPath 4000 gateways (HG35xx)
- extend the capabilities for secure operation of the gateways (Gateway Secure Mode)

We recommend that all customers update their HiPath 4000 systems accordingly and apply the supported hardening capabilities in accordance with the customer's individual security policy or requirements.

Vulnerability Details

The update is a backport of existing capabilities in OpenScape 4000 V7 to ensure that extended security posture of V7 gateways is made available to users of HiPath 4000 V6 as well.

The update covers the resolution for:

- CVE-2010-4180 ("SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG")
- Elimination of weak and medium strength ciphers in the https interface of the gateways
- Disable outdated SSL protocol versions (up to and including SSLv3)
- Gateway secure mode: limit the web-based access to the gateways via the HiPath 4000 Assistant only.
  For details and further hardening options refer to the latest issue of the HiPath 4000 V6 Security Checklist, chapter "Security Mode Configuration".

Note: In addition to these security improvements we also recommend to install customized and trusted X.509v3 certificates for the web interfaces (https on HiPath 4000 Assistant and Gateways). This enables Browsers and any 3rd party https clients to properly authenticate the web server when accessing the HiPath 4000. For more information refer to the chapter "Remote Administration via HTTPS" in the Security Checklist.
In this context, this update of the HiPath 4000 V6 R2 gateway software also adds support for X.509v3 certificates signed with the SHA-2 hash algorithm. We recommend to use SHA-2 signed server certificates for all TLS interfaces of HiPath 4000. Certificates signed with the older SHA-1 or MD5 algorithms should be considered as weak. They could potentially undermine the confidentiality or integrity of the data exchanged in a specific TLS connection.

Affected Products

- HiPath 4000 V6

Recommended Actions

- Install HiPath 4000 IP gateway loadware version in the HiPath 4000 Specific LW-Hoftix 2 for V6 R2.16.0 (HF003771, release date: 2014-07-03) or later
- Apply the recommended hardening measures as listed in the HiPath 4000 V6 Security Checklist (issue 3, released: 2014-07-21) and as appropriate and aligned with the individual customer's security policy and requirements.

References

External links:

- Mitre: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4180

Unify:

- HiPath 4000 V6 Security Checklist, issue 3 (A31001-H3160-P101-3-7620, 07-2014)

Revision History

2014-07-23: Initial release

Advisory ID: OBSO-1407-02 (a=83), status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer
OpenScape Baseline Security Office
obso@unify.com

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