Security Advisory Report - OBSO-1401-03

HiPath 4000/OpenScape 4000 - Unauthenticated write access to file system

Creation Date: 2014-01-31
Last Update: 2014-01-31

Summary

A vulnerability in the NFS configuration of HiPath 4000 V6 R2 and OpenScape 4000 V7 was reported that allows unauthenticated remote attackers to upload arbitrary files to the system.

The risk is rated **medium** (CVSS Base Score: 5.8).

Vulnerability Details

This vulnerability is only relevant when separated duplex systems are deployed.
It affects the associated quorum server, where the unprotected NFS share is provided.

Attackers may exploit this vulnerability by uploading or modifying files on the server. This could potentially be used to launch further attacks that affect the availability, integrity or confidentiality of the HiPath/OpenScape 4000 solution.

Affected Products

- HiPath 4000 V6 R2
- OpenScape 4000 V7

Earlier versions of HiPath 4000 are not affected.

Recommended Actions

To solve the vulnerability, upgrade the HiPath/OpenScape 4000 platform (Novell SLES):

- HiPath 4000 V6 R2 to V6 R2.15.1 (Hotfix HF003496, released: 2013-12-06) or later
- OpenScape 4000 V7 to V7 R0.12.2 (Hotfix HF003497, released: 2013-12-23) or later

Recommended mitigation measures for existing installations:

- Disable the NFS share on the quorum server
- Connect the quorum server via the Corosync LAN, instead of the Customer LAN

References

N.A.

Revision History

2014-01-31: Initial release

Advisory ID: OBSO-1401-03 (a=67), 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