Security Advisory Report - OBSO-1010-02

Arbitrary code execution at Manager -E

Creation Date: 2010-10-15
Last Update: 2010-10-26

Summary

A vulnerability was discovered in Manager-E that allows to execute arbitrary code on the victim client, where Manager-E is installed.

Vulnerability Details

The vulnerability can be exploited by tricking the user to open a crafted .kds file.

At least Manager-E V7 and V8 are affected.

Affected Products

- HiPath 3000/5000 Manager E, version V8 R4 and lower

Recommended Actions

Do not open .kds Files with HiPath 3000/5000 Manager E which you have received from untrusted sources.

Upgrade Manager E to V8 R5.0.0 or higher, which are not affected by this vulnerability.

Note that opening a corrupt .kds file may cause the application to crash.

References

None.

Credits: We like to thank Sofiane Talmat for reporting this issue.

Revision History

2010-10-15 Initial release
2010-10-26 Fix release number corrected

Advisory ID: OBSO-1010-02 (a=3), status: update 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