Security Advisory Report - OBSO-1407-01

NTP Distributed Reflection Denial-of-Service (DRDoS) attack via the monlist feature (CVE-2013-5211)

Creation Date:	2014-07-25
Last Update:	2014-07-25

Summary

The monlist feature in the network time protocol (NTP) daemon on Linux servers allows remote attackers to cause a denial of service (traffic amplification) via forged requests.

This advisory summarizes the impact of the vulnerability for customers using products of Unify and the recommended countermeasures.

The risk is rated as medium.

Vulnerability Details

NTP is designed for time synchronization, and may also implement other features such as server administration, maintenance, and monitoring. NTP relies on the user datagram protocol (UDP) to send and receive messages, which does not validate the source (IP address) of the sender.
In an NTP DRDoS attack the attacker sends a packet with their source address being the IP of a victim. The NTP server replies to this request, but the number of bytes sent in the response is an amplified amount compared to the initial request, resulting in a denial-of-service on the victim.
(Source: US-CERT)

Mitre (cve.mitre.org) has assigned the id CVE-2013-5211 to this issue.
CVSS v2 Base Score for affected Unify products: 5.0 (AV:N/AC:L/AU:N/C:N/I:N/A:P)

Affected Products

The following products of Unify are delivered with a potentially vulnerable default configuration of the NTP server:

- OpenScape Office MX V3 before V3 R3.10.0
- HiPath 4000 V6: Assistant (before V6 R2.42.4) and CSTA (before V1 R13.203.1)
- OpenScape 4000 V7: Assistant (before V7 R0.14.5) and CSTA (before V7 R0.205.3)

Recommended Actions

Install the following Unify product releases (or later versions) to resolve the vulnerability:

- OpenScape Office MX: V3 R3.10.0 (release date: 2014-06-12)
- HiPath 4000 V6:
  - Assistant: V6 R2.42.4 (release date: 2014-07-25)
  - CSTA: V1 R13.203.1 (release date: 2014-06-06)
- OpenScape 4000 V7:
  - Assistant: V7 R0.14.5 (release date: 2014-07-15)
  - CSTA: V7 R0.205.3 (release date: 2014-06-06)

Note that for HiPath/OpenScape 4000, the update will completely disable the NTP service by default, as it is not required for proper operation of the system.

Recommendation for Linux-based applications of Unify
(such as OpenScape UC application servers, Media Server, Common Management Platform, OpenScape 4000 Manager, OpenScape Business S/Booster Server, OpenScape Office LX/HX, OpenScape Xpert System Manager):

- Applications installed on Novell SUSE Linux Enterprise Server: apply the hardening recommendations as provided by Novell (https://support.novell.com/security/cve/CVE-2013-5211.html. There are no known restrictions or other side effects known for Unify application products
- Applications installed on Debian Linux (OpenScape Xpert Multi Line Controller only): no explicit actions necessary, as the default installation of Debian Linux is not susceptible to CVE-2013-5211
- ntp.org provides a comprehensive guide for secure operation of NTP servers at: http://support.ntp.org/bin/view/Support/AccessRestrictions

References

External links:

- Mitre: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5211
- NVD: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-5211
- ntp.org: Security Notice for CVE-2013-5211 and NTP hardening guide
- Novell: https://support.novell.com/security/cve/CVE-2013-5211.html
- US-CERT: http://www.kb.cert.org/vuls/id/348126

Revision History

2014-07-25: Initial release

Advisory ID: OBSO-1407-01 (a=81), 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

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.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.