UNIFY

Security Advisory Report - OBSO-1607-01

httpoxy: A CGI Application Vulnerability Affecting Multiple Web Application Languages and Services

Creation Date: 2016-07-21
Last Update: 2016-07-27

Summary

On July 18th, 2016 a vulnerability in Common Gateway Interface (CGI) environments was disclosed. It could affect any web application that is based on scripting languages (such as PHP, Go, Python) and/or web servers (such as Apache HTTP server, Apache Tomcat).
Mitre and the DWF project have assigned various CVE-IDs, depending on the way individual software components are impacted. The vulnerability was named "httpoxy".

This advisory summarizes the impact of "httpoxy" for customers using products of Unify.
Risk for Unify products: none (*)
Unify products are considered as not vulnerable.

(*) So far, no vulnerability in Unify products could be identified. The advisory will be updated if new information becomes available.

Vulnerability Details

The vulnerability is caused by a name clash between a CGI environmental variable ("HTTP_PROXY") and a web client's ability to set a "Proxy: " header value with any HTTP request, that is - on the web server - being converted into a variable of the same name ("HTTP_PROXY"). Therefore, **if**

- an attacker sends an arbitrary value for the "Proxy: " header value, pointing to a HTTP Proxy server under the attacker's control, **and**
- the victim web server application is executing any HTTP requests to further web services, while considering the (modified) setting of the HTTP Proxy server address,

then the attacker may be able to read and modify all (or parts of) the communication between the web application and the web service the application is requesting.

For more details refer to the disclosure site: https://httpoxy.org/ and further documents listed in the "References" section.

Affected Products

The following Unify products are confirmed as **not** affected by "httpoxy":

- OpenScape Voice, OpenScape Branch, OpenScape SBC
- OpenScape 4000 (Platform, Softgate, Assistant, CSTA) and OpenScape 4000 Manager
- OpenScape UC Application (all components, incl. Web Client, Frontend/Backend, Media Server, Facade Server)
- OpenScape Web Collaboration
- OpenScape Xpressions
- OpenStage / OpenScape Desk Phone IP / CP devices
- OpenScape Management Applications: Common Management Platform, Deployment Service, Fault Management, **Accounting Management**
- OpenScape Contact Center (OSCC) Agile/Enterprise, OSCC CDSS and OSCC Extensions
- OpenScape License Management
- Diagnosis Applications: OpenScape Voice Trace Manager, OpenStage Diagnostic Data Collector
- **OpenScape Xpert**
- **OpenScape Business and OpenScape Office**

Recommended Actions

No specific actions are necessary or recommended in the context of Unify products.

References

- httpoxy "landing page": https://httpoxy.org/
- CERT/CC Vulnerability Note VU#797896
- Associated advisory by the Apache Software Foundation: https://www.apache.org/security/asf-httpoxy-response.txt

Revision History

2016-07-21: Initial release

2016-07-27: Update 01

- Added OpenScape Accounting Management, OpenScape Xpert, OpenScape Business and OpenScape Office to the list of unaffected products