Security Advisory Report - OBSO-1409-01

Bash - Remote Command Injection Vulnerability "Shellshock" (CVE-2014-6271, CVE-2014-7169 et al.)

Creation Date:	2014-09-27
Last Update:	2015-07-28

Summary

On September 24, 2014, a vulnerability in the Unix shell implementation 'bash' (GNU Bourne Again Shell) was disclosed that affects many products and online services in the Internet. It affects Unix-based systems, including Linux and Mac OS X and is also known as "Shellshock".
This advisory summarizes the impact of this vulnerability for customers using products of Unify.

Risk for Unify products:
Rated as high for HiPath/OpenScape 4000 (Platform, Assistant, Softgate) and for HiPath/OpenScape 4000 Manager.
Other Unify products are only affected with low risk or not affected at all.
See the product-specific details in the section "Affected Products" below.

Update note 2014-10-23:
Official solutions are now available for all Unify products that are affected with high risk.
Further advisory updates are expected to cover release information for products affected with low or no risk only.

Vulnerability Details

Vulnerable versions of 'bash' may allow remote attackers to execute arbitrary Unix shell commands on the target system by overriding or bypassing environment restrictions caused by flaws in the function parsing implementation of bash.
For a detailed description please refer to the references section below.

Mitre (cve.mitre.org) has assigned the id **CVE-2014-6271** to this issue.
Note that patch releases for 'bash' were already provided by various Linux distributions (incl. Novell SLES, Debian Linux), which do not solve the issue completely. Therefore, additional ids (**CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, CVE-2014-6278**) were created. They describe additional flaws related to the same type of "Shellshock" vulnerabilities and track the succeeding corrections in the bash function parsing.
Also (without associated CVE number) an additional hardening implementation was done in 'bash'. The **"hardening fix"** is expected to close this issue completely. It prevents that potential further (yet unknown) flaws in the function parser implementation of 'bash' become relevant as additional "Shellshock" vulnerabilities.

From our current point of view,

- **CVE-2014-6271 describes the vulnerability with the highest risk** and requires immediate countermeasures for systems that are seriously impacted. For details regarding affected Unify products see below
- CVE-2014-7169 rates as medium risk and (if at all) is only relevant for Unify products, where CVE-2014-6271 is relevant, too. So far however we have no evidence that any of the Unify products is affected. An exploitation is unlikely
- CVE-2014-7186 and CVE-2014-7187 are not relevant for Unify products
- CVE-2014-6277 and CVE-2014-6278: the details have been disclosed on 2014-10-01;
  CVE-2014-6278 **is considered similarly critical for Unify products as CVE-2014-6271**.

All CVEs are resolved as part of the "Hardening fix"; therefore the "Hardening fix" is considered with the same priority as the original fix (for CVE-2014-6271).

Affected Products

1. Vulnerable:

The following Unify products are affected by CVE-2014-6271 et al.

1.1 Vulnerable with high risk:

1.1.1 HiPath/OpenScape 4000 - Platform and Softgate (all versions V6 Rx and V7 Rx)

Various links provided at the web interface (https / port 443) allow arbitrary code execution on the server without prior authentication.

CVSS Base Score: 9.0, CVSS Temporal Score: 8.1
CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:P/A:C/E:F/RL:W/RC:C)

Solution available for V6:

- **V6 R2.16.0 - Softgate and Platform:**
  Install LW Hotfix 5 - HF003895 and PLT Hotfix 3 - HF003892 (GA release date 2014-10-17)
- **Interim solution for V6 R1:** HiPath 4000 V6 R1 has already achieved end of SW support; to extend the time window for planned upgrades to V6 R2, an interim solution is provided for the latest version of V6 R1 (Platform V6 R1.12.2, Assistant V6 R1.13.11).
  For details refer to the Unify Knowledgebase article ID 223411 (release date 2014-10-09).
  Note that this interim solution only solves the bash/shellshock vulnerability, while various other security improvements (including but not limited to those described in OBSO-1407-01) remain unresolved in V6 R1.

Solution available for V7 R1:

- **V7 R1.8.0 - Softgate: Install LW Hotfix 3 - HF003896** (GA release date 2014-10-17)
- **V7 R1.8.0 - Platform: Install PLT Hotfix 2 - HF003893** (GA release date 2014-10-23)

1.1.2 HiPath/OpenScape 4000 - Assistant (all versions V6 Rx and V7 Rx)

Various links provided at the web interface (https / port 443) allow arbitrary code execution on the server without prior authentication.
CVSS Base Score: 7.5, CVSS Temporal Score: 7.1
CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:P/A:P/E:F/RL:ND/RC:C)

Solution available:

- **for V7: install Hotfix V7 R1.7.3 - HF003886** (GA release date 2014-10-02)
- **for V6: install Hotfix V6 R2.42.5 - HF003894** (GA release date 2014-10-20)

1.1.3 Hipath/OpenScape 4000 - Manager (all versions V6 Rx and V7 Rx)

Various links provided at the web interface (https / port 443) allow arbitrary code execution on the server without prior authentication.
CVSS Base Score: 7.5, CVSS Temporal Score: 6.2
CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C)

Solution available - apply the following Novell patch for SUSE Linux Enterprise Server at the earliest opportunity (in accordance with the individual customer's patch and update processes and schedule):

- CVE-2014-7169 (release date: 2014-09-28)
  This accumulates the solution/mitigation for all related vulnerabilities in 'bash' and also includes the "hardening fix

1.2. Vulnerable with low risk

1.2.1 OpenScape UC Applications - Common Management Platform (CMP - all versions)

One link provided at the web interface (https / port 443) may allow arbitrary code execution on the server, requiring prior authentication at the CMP with administrative access rights.
This only applies to UC servers, where CMP is available: CMP standalone (i.e. Multiple Communication Server Admin), Media Server standalone and UC Backend server.
Other installations of UC Applications (such as UC Frontend server, Facade server, Media server as part of a UC large deployment) are not affected.
CVSS Base Score: 4.6, CVSS Temporal Score: 3.7
CVSS v2 Vector (AV:N/AC:H/Au:S/C:P/I:P/A:P/E:U/RL:W/RC:C)

Solution available - apply the following Novell patch for SUSE Linux Enterprise Server (in accordance with the individual customer's patch and update processes and schedule):

- CVE-2014-7169 (release date: 2014-09-28).
  This accumulates the solution/mitigation for all related vulnerabilities in 'bash' and also includes the "hardening fix"

1.2.2 OpenScape Voice (all versions)

The OpenScape Voice Server (OSV) is not affected, except for OSV integrated simplex installations, where the Common Management Platform (CMP) is installed and operated on the OSV. This results in the same impact and risk rating as in 1.2.1 above.
CVSS Base Score: 4.6, CVSS Temporal Score: 3.7
CVSS v2 Vector (AV:N/AC:H/Au:S/C:P/I:P/A:P/E:U/RL:W/RC:C)

Solution available:

- for V8: update to V8 R0.34.3 - fix is included in MOP Q3061 (GA release date 2014-12-19)
- **for V7: update to V7 R1.42.2 - fix is included in MOP Q3059** (GA release date 2015-01-06)

1.2.3 OpenScape Business (all versions)

OpenScape Business is affected in two ways, both are rated as low risk:

- One link provided at the administration interface (web-based management - WBM, https / port 443) may allow arbitrary code execution on the server, requiring prior authentication with administrative access rights. No other interfaces (incl. UC clients access: myPortal, myAttendant etc.) are affected.
  CVSS Base Score: 4.6, CVSS Temporal Score: 3.7
  CVSS v2 Vector (AV:N/AC:H/Au:S/C:P/I:P/A:P/E:U/RL:W/RC:C)
- When DHCP is configured for the administration and/or the WAN interface, a malicious DHCP server in the customer's network may execute arbitrary code on the OpenScape Business server. DHCP is disabled by default, therefore standard installations of OpenScape Business are not affected.
  CVSS Base Score: 3.7, CVSS Temporal Score: 3.2
  CVSS v2 Vector (AV:A/AC:H/Au:M/C:P/I:P/A:P/E:F/RL:TF/RC:C)

Solution available for:

- **OpenScape Business X1/X3/X5/X8: update to version V1 R3.2.0 (release date 2014-10-24)**
- OpenScape Business S and UC Booster Server:
  Apply the following Novell patch for SUSE Linux Enterprise Server (in accordance with the individual customer's patch and update processes and schedule):
  - CVE-2014-7169 (release date: 2014-09-28).
    This accumulates the solution/mitigation for all related vulnerabilities in 'bash' and also includes the "hardening fix"

1.2.4 OpenScape Office (all versions)

OpenScape Office is affected in two ways, both are rated as low risk. The issues are the same as for OpenScape Business, please refer to section 1.2.3 for details.

Solution available for:

- OpenScape Office MX: update to version V3 R3.11.0 (release date 2014-10-17)
- OpenScape Office HX and LX:
  Apply the following Novell patch for SUSE Linux Enterprise Server (in accordance with the individual customer's patch and update processes and schedule):
  - CVE-2014-7169 (release date: 2014-09-28).
    This accumulates the solution/mitigation for all related vulnerabilities in 'bash' and also includes the "hardening fix"

1.2.5 OpenScape Branch and OpenScape SBC

Important update 2014-10-06:
Additional investigation and tests have identified an impact to both products. A potential risk however only exists in a small time window during server restarts. Stable and running servers are not affected.
CVSS Base Score 5.1, Temporal: 4.8
CVSS v2 Vector (AV:N/AC:H/Au:N/C:P/I:P/A:P/E:F/RL:U/RC:C)

Solution available - install the following patches (all released on 2014-10-10):

- OpenScape Branch V8 R0.5.1 (08.00.05.00-3 Patch 01)
- OpenScape Branch V7 R1.22.1 (07.01.22.02 Patch 01)
- OpenScape SBC V8 R0.5.1 (08.00.05.00-3 Patch 01)
- OpenScape SBC V7 R1.22.1 (07.01.22.01 Patch 01)

1.2.6 OpenScape/HiPath CAP V3.0

CAP V3.0, although a Windows-based server application, shipped a vulnerable version of bash as part of the HBR (backup/restore) package until version V3.0 R13. The risk is rated low.
CVSS Base Score 4.6, Temporal: 3.4
CVSS v2 Vector (AV:N/AC:H/Au:S/C:P/I:P/A:P/E:U/RL:OF/RC:C)

Solution available: Upgrade to CAP V3.0 R14.x.x (released on 2014-07-30) or higher, where the HBR package is no longer in use or accessible.

1.2.7 OpenScape Contact Center Call Director (CDSS)

Important update 2014-10-16: CDSS is affected with low risk:

- When DHCP is configured, a malicious DHCP server in the customer's network may execute arbitrary code on the CDSS appliance. To mitigate, disable DHCP on CDSS and use static IP address configuration instead.
  CVSS Base Score: 4.3, CVSS Temporal Score: 3.7
  CVSS v2 Vector (AV:A/AC:H/Au:N/C:P/I:P/A:P/E:F/RL:TF/RC:C)

Solution available:

- Update 2014-10-25: A patch release for CDSS V8 R2 versions before V8 R2.10 can be retrieved now via GCS/GVS. Please check the

Customer Support Portal for general availability of the patch (available soon on SW supply server - Direct link)
- **Update 2015-07-28: The official correction is available in CDSS V8 R2.10.11192 (release date 2015-07-24, see Service information INF-15-000323.**
  We recommend all customers to upgrade CDSS to this version, as it contains corrections for multiple other security vulnerabilities as well.

2. Not vulnerable:

The following Unify products are confirmed as not being affected:

- **All products running on MS Windows** operating system (for example OpenScape Xpressions, OpenScape Deyployment Service, OpenScape Contact Center, OpenScape Xpert System Manager, Partner product: ASC EVOip Windows (*)
  (*) Note regarding ASC EVOip Linux (not released for use in Unify solutions): There is no evidence that the vulnerability can be leveraged on ASC's Linux-based products - nevertheless, as a precautionary measure the appropriate updates of the bash package ***have been included as part of a service pack, released on 2014-11-10.*** *For up-to-date information, refer to ASC's statement at:* http://asc.de/english/partners.html
- **All gateways running on VxWorks** operating system (for example RG 8700, HiPath/OpenScape 4000 Gateways HG35xx, HiPath 3000 Gateway HG1500)
- **Linux-based products (SW appliances) that don't include 'bash':**
  - OpenStage and OpenScape Desk Phone IP phones
  - HiPath Cordless IP
  - OpenScape Alarm Response Eco and Pro 200
  - Partner Product: Media5 Mediatrix Gateways
- **Linux-based Software appliances, that ship an affected version of 'bash'**
  (in other words, well-known tests such as:
  env x='() { :;}; echo vulnerable' bash -c ":"
  report "vulnerable" on the appliance):
  There is no evidence that the vulnerability can be leveraged on these appliances - nevertheless, as a precautionary measure the appropriate updates of the bash package will be included as part of the regular cycle of maintenance releases.
  - OpenScape Voice (non-integrated, w/o CMP): see chapter 1.2.2 above for release information
  - **CSTA V1 R13 in HiPath 4000 V6 R2:**
    The update is included in the hotfix version V1 R13.203.3 - HF003907, release date: 2014-11-03
  - **CSTA V7 R1 in HiPath 4000 V7 R1:**
    The update is included in the hotfix version V7 R1.206.2 - HF003915, release date: 2014-11-17
  - OpenScape Alarm Response Pro 300
- **Linux-based Server applications:**
  The Linux Operating Systems, where the following applications are installed on, contain 'bash' and are inherently vulnerable, if not patched.
  There is however no evidence that the vulnerability can be leveraged through the Unify application, if installed and operated in accordance with the associated administration manuals, security checklists and release notes.
  As a precautionary measure we recommend to apply the relevant Operating System patches (in accordance with the individual customer's patch and update processes and schedule) as specified.
  - OpenScape UC Application Facade Server, Media Server, UC Front-End/Back-End Server, OpenScape Voice Survival Authority
    Solution: apply Novell patch for SUSE Linux Enterprise Server as specified in CVE-2014-7169 (release date: 2014-09-28).
  - OpenScape Xpert Multi-Line Control Server (MLC)
    Solution: apply patch for Debian 7 (wheezy) as specified in dsa-3035 (release date: 2014-09-25)

3. End of life products

Unless specified explicitly, all versions of the listed products are included that are in the phase between general availability (GA) and end of life (EOL).
Products or product versions that are beyond EOL are typically not considered in security advisories.
Important Note: There is evidence that **HiPath 4000 V5 and lower** (all beyond EOL) are also vulnerable to CVE-2014-6271 et al.
We recommend all customers still running V5 or lower to upgrade to V6 R2 or V7 R1 and apply the patches as soon as released.
In cases where this is not possible in short term:

- All older versions of HiPath 4000: ensure that the access to the Webinterface (https / port 443) of **Assistant** is limited to trusted system administrators only, or turned off.
- HiPath 4000 V5 only: **Softgate** was introduced with V5, but unlike in V6 and later (where the Softgate is provided as a SW appliance), the Softgate in V5 was an application delivery based on Novell SLES 11. Customers may apply the patches as released by Novell at own risk.

Recommended Actions

This chapter focuses on the products, that are impacted with high risk.
Apply the proposed countermeasures as appropriate and at least until the solution is available and has been installed on your systems.

For HiPath/OpenScape 4000:
Ensure that the access to the Webinterfaces (https / port 443) of **Assistant, Platform and Softgate** is limited to trusted system administrators only ***(*)***.
This is the only vulnerable remote interface provided by the 4k systems.
Additionally, consider applying the following countermeasure for **Platform and Softgate:**

- Precondition: Ensure that you have installed one the following versions or higher:
  V7 R1 (any fix release), LW HF V7 R0.12.4, or LW HF V6 R2.16.2
- Use the Assistant to enable "**Gateway Secure Mode**" for both Platform and Softgate as recommended in chapter 4.7 of the OpenScape 4000 Security Checklist

HiPath/OpenScape 4000 Manager:
A solution is already available, see section "Affected Products".
As a general best-practice measure for management applications, ensure that the access to the Webinterface (https / port 443) is limited to trusted system administrators only ***(*)***.
In the context of this advisory, this interface is the only vulnerable remote interface provided by the HiPath/OpenScape 4000 Manager.

(*) General note:
The available options to limit the access to vulnerable systems on network level depend on the individual customer's network setup and infrastructure. Potential countermeasures include, but are not limited to:

- *establish a separate Admin-VLAN/LAN, or even a local subnet only for administrative purposes*
- *configure firewalls to restrict the access to only trusted IP addresses*
- *in cases where Web Application Firewalls (WAF) and/or IDS/IPS systems are in use: use the vendor-specific updates, signatures or rules to detect / prevent network attacks that try to exploit this vulnerability.*

References

Description of the "shellshock" vulnerabilities:

- RedHat Security Blog Entry
- US-CERT Vulnerability Note VU#252743

Mitre:

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278

NVD:

- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6278

Solutions for Application Servers:

- Novell SUSE Linux Enterprise Server: CVE-2014-7169 (release date: 2014-09-28)
- Debian 7 (wheezy): DSA-3035-1 (release date: 2014-09-25)

Revision History

2014-09-27: Initial release
2014-09-29: Update 01

- Added new "Shellshock" related vulnerabilities (CVE-2014-6277, CVE-2014-6278)
- Added statement regarding EOL products, especially HiPath 4000 < V6
- Completed solution for application servers (apply both patches for Novell SLES)
- Revised section "Recommended Actions"

2014-10-02: Update 02

- Important:
  - Final solution available for OpenScape 4000 Assistant V7
  - Preliminary patches available for all other HiPath/OpenScape 4000 systems and versions
- Added statements for/impact to:
  - OpenScape Business, OpenScape Office and HiPath 3000
  - HiPath 4000 CSTA
  - OpenScape Contact Center CDSS
  - Mediatrix Gateways
- Errata: fixed two incorrect CVE numbers in the section "Vulnerability details"
- Errata: fixed CVSS temporal score for products affected with low risk (3.7 instead of 3.4)
- Additional information and categorization in the list of not affected products
- Clarification that the Novell patch for CVE-2014-7169 is cumulative
- Focus of the section "Recommended Actions" on products affected with high risk; listed proposals how to limit access to vulnerable systems
- EOL products: added a note regarding Softgate in HiPath 4000 V5
- Extended section "References"

2014-10-06: Update 03

- Update of risk analysis for OpenScape Branch and for OpenScape SBC: risk for both raised from "no risk" to "low"
- Added HiPath/OpenScape CAP V3.0 (affected with low risk in versions before V3.0 R14)
- Added expected plan dates for fix releases in OpenScape Business and OpenScape Office

2014-10-10: Update 04

- Important:
  - HiPath 4000 V6 R2: solution available for Platform and Softgate
  - Interim solution provided for HiPath 4000 V6 R1
  - OpenScape 4000 V7 R1: solution available for Softgate
- Solution available for OpenScape Branch V7 R1 / V8, and for OpenScape SBC V7 R1 / V8
- Included status information for ASC EVOip

2014-10-13: Update 05

- Important: HiPath 4000 V6 R2: solution available for Assistant
- Errata: clarification of the impact to the various deployments of Common Management Portal; fixed a typo in the HiPath 4000 number

2014-10-16: Update 06

- Reviewed risk rating for OpenScape Contact Center Call Director SIP Service (changed to 'low'), incl. mitigation measures and release plan

2014-10-17: Update 07

- Important:
  - HiPath 4000 V6 R2: solution released for Platform and Softgate (GA)
  - OpenScape 4000 V7 R1: solution released for Softgate (GA);
solution available for Platform in status Pilot Usage
- Solution released for OpenScape Office MX
- Added status information for CSTA V1 R13 in HiPath 4000 V6 R2

2014-10-21: Update 08

- HiPath 4000 V6 R2: solution released for Assistant (GA)

2014-10-23: Update 09

- OpenScape 4000 V7 R1: solution released for Platform (GA)
- Added note: Official solutions are now available for all products that were affected with high risk.

2014-10-25: Update 10

- Solution released for OpenScape Business and for OpenScape Contact Center Call Director SIP Service (CDSS)

2014-12-23: Update 11

- chapter 1.2.2: Solution released for OpenScape Voice V8
- chapter 2: Completed release information for the CSTA component in HiPath/OpenScape
- *chapter 2: updated statement for partner product ASC EVOip Linux*

2015-01-21: Update 12

- chapter 1.2.2: Solution released for OpenScape Voice V7 R1
- chapter 2: Added OpenScape Voice Survival Authority to the list of application server products that are not affected by "shellshock"

2015-07-28: Update 13

- chapter 1.2.7: Solution released for **OpenScape Contact Center CDSS V8 R2**

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.