Security Policy

Vulnerability Intelligence Process

Version: 1.2.2
Date: 2019-04-03

OpenScape Baseline Security Office
Unify Software and Solutions GmbH & Co. KG

1. Overview

A key requirement for the products, services and solutions delivered by Unify Software and Solutions GmbH & Co. KG (Unify) is security. It is best engineering practice for security measures to be built in, not bolted on.

Unify supports this requirement by using a comprehensive security software development lifecycle that applies to all new Unify products or product versions being developed.

Although constant care is taken during the software development, security vulnerabilities may still emerge after a Unify product was released.

This policy describes the Vulnerability Intelligence Process (VIP) at Unify.

It regulates how to

- identify, analyse and resolve security vulnerabilities in released Unify products, and
- deliver guidance to customers how to mitigate or close these vulnerabilities.

1.1. History of Change

Date	Version	What
2012-06-27	1.0	Initial release
2013-11-11	1.1	Update release (company rebrand, organisational changes)
2016-02-01	1.2	• Chapter 1.4: updated product list; added reference to Unify's Product Lifecycle Policy • Chapter 2.3.2: update from CVSS version 2 to version 3 • Chapter 2.4: added public URL to access Unify Security Advisories • Chapter 3.4: updated PGP encryption key Various editorial changes
2018-05-23	1.2.1	Update Logo, remove PGP
2019-04-03	1.2.2	Replace obso@unify.com with obso@atos.net

1.2. Table of Contents

1.3. Baseline Security Policy

The Vulnerability Intelligence Process (VIP) is an integral part of the Baseline Security Policy at Unify. In addition to the ISO 9001 certified software development process, the Baseline Security Policy contains the technical guidelines for the secure development, release and sustaining of the company's products. It defines the fundamental measures for software security that are taken throughout the whole lifecycle of a product:

- Product planning and design:
  Threat and risk analysis (**Theoretical Security Assessment**) to determine the essential security requirements for the product
- Product development and test:
  Penetration tests (**Practical Security Assessment**) to discover implementation vulnerabilities and to verify the hardening of the default system configuration
- Installation and start of operation:
  Hardening guides (**Security Checklists**) to support the configuration of the systems according to the individual customer's security policy
- Operation and maintenance:
  Proactive **Vulnerability Management** to identify, analyze and resolve security vulnerabilities that emerge after products have been released, and to deliver guidance to customers how to mitigate or close these vulnerabilities

1.4. Applicability of the Vulnerability Intelligence Process

In the current version, the process applies to the following product areas provided by Unify:

- Voice platforms including gateways (such as OpenScape Voice/Branch/SBC, OpenScape 4000, OpenScape Business)
- OpenScape applications (such as UC Applications, Xpressions, Web Collaboration)
- OpenScape Management applications (such as Common Management Platform, Deployment Service, Fault Management, Accounting Management, OpenScape 4000 Manager)
- End-user devices and applications (such as OpenStage and OpenScape Desk Phone CP phones, OpenScape UC desktop applications and mobile apps, Circuit apps)
- OpenScape Contact Center
- OpenScape Xpert

All products that belong to these areas are actively monitored for potential vulnerabilities, from the first day they have been released, until their End of Standard Support (M44). After M44, customers may negotiate an extension through Extended Manufacturer Software Support (EMSS – see [1]).

2. Vulnerability Intelligence Process (VIP)

The VIP is within the responsibility of the OpenScape Baseline Security Office (OBSO) at Unify. The OBSO is a global team that, among other tasks, defines and executes the process defined in this document.

The scope of the VIP is explained in chapter 2.1. The following chapters describe the key elements of the VIP in detail:

- Permanent monitoring of new and updated security vulnerabilities
- Assessment of their impacts to Unify products and evaluation of countermeasures
- Guarantee that the current security checklist is part of the installation instructions of the product documentation
- Notification of customers and users about potential risks

2.1. Definition and Scope

2.1.1. Definition of "Product Security Vulnerability"

The VIP primarily deals with "product security vulnerabilities".

In the context of this document, "**product security vulnerability**" is defined as a flaw in a software product of Unify that impairs the product's designed and available capabilities with regard to confidentiality, integrity or availability.

In most cases it therefore requires a new software release or a patch, to be delivered by Unify, to finally solve a "**product security vulnerability**".

The remaining part of this chapter lists some examples of what is **not** considered as a "product security vulnerability":

- The vulnerability can be solved by user-individual or administrative hardening steps.
  A very common example is the use of default passwords instead of choosing individual, complex ones. It is still the case that a significant percentage of all successful attacks are based on unauthorized access to systems by using the factory default settings.
- Intentional use of a feature or configuration setting that is weaker than current security best-practice.
  In many situations, a trade-off between security and other interests (such as ease of use, performance, operational costs) may be made. For example, communication in clear text may be configured between two systems residing in the same network segment to speed up the data transfer.
- The (designed or intentional) lack of a product security capability.
  For example, if a product has implemented only one administrative role or level. The risk is that every user of the product may exceed their privileges by being able to modify data, although not authorized. This is not a vulnerability of the existing product but requires a feature enhancement in a follow-up version of the product.

2.1.2. Scope of the VIP

The key deliverable of the VIP is to provide customers with reasonable and useful vulnerability information (called Security Advisories, see chapter 2.4) which they can consider in their own vulnerability assessment and patch processes.

A security vulnerability can usually be assigned to one of the following three categories:

Cat. 1 - The vulnerability is part of software developed by Unify and included in one or more Unify products
Cat. 2 - The vulnerability is caused by a 3rd-party software component that is embedded in one or more Unify products
Cat. 3 - The vulnerability is caused by the environment, where Unify products operate (such as Operating Systems, where an application has been installed, or products of other vendors, which Unify products are connected with)

Clearly, **the VIP applies to Cat. 1** vulnerabilities. Customers should consider the VIP in their individual vulnerability and patch management processes.

The VIP does not apply to Cat. 3 vulnerabilities. To consider Cat. 3 vulnerabilities in vulnerability and patch management processes refer to the corresponding vendor's security advisories and software release cycles, as well as compatibility matrices that are relevant to the customer's individual solution setup.

Cat. 2 vulnerabilities may either belong to the VIP or not: it depends on the individual 3rd-party software component embedded in a product, and whether the component can be updated or patched by customers without having to wait for a new fix release of the whole product. This is usually described in an individual product's documentation or release note. If there is uncertainty for a specific product, ask your service or sales representative at Unify for clarification.

The following figure marks the typical border, where the closure of a security vulnerability requires a new fix release or a patch delivered by Unify.

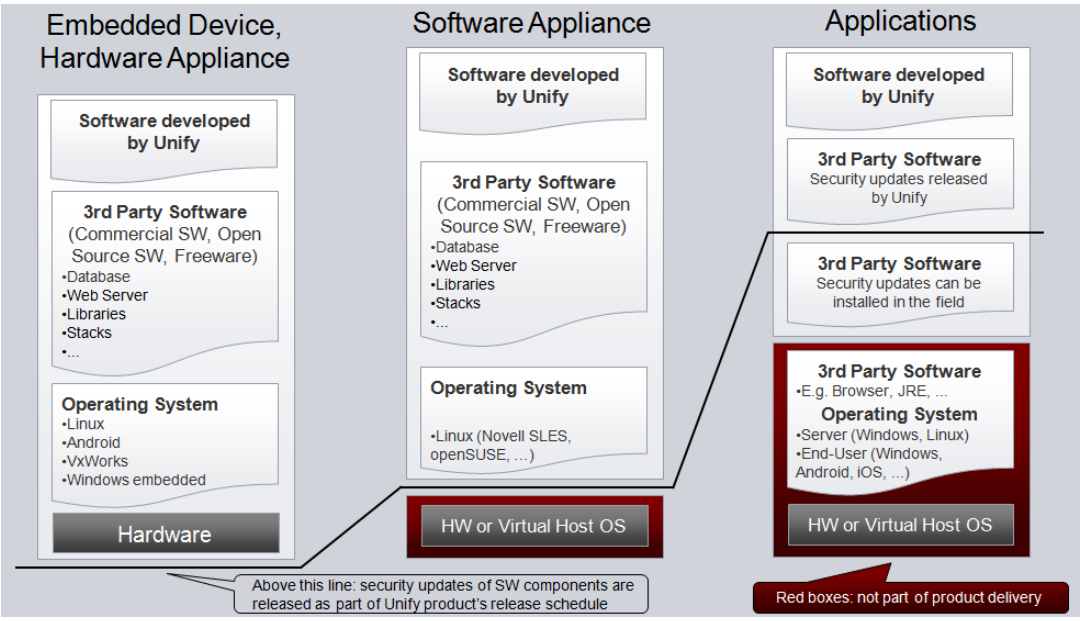

Figure 1 – Product types and applicability of security updates

2.2. Active Monitoring

The following sources are monitored for security vulnerabilities that are potentially affecting Unify products:

- Vulnerabilities that become known to the public through various sources, especially through software vendor advisories, CERT (Computer Emergency Response Team) and governmental organizations, and professional vulnerability information service providers[1]. Vulnerability information is consolidated among different sources, pre-analyzed in detail, kept up-to-date and delivered quickly to the relevant product teams.The potential relevance and impact of a public vulnerability is determined immediately after, based on the products' lists of incorporated 3rd party software components.
- Results of internal security assessments (according to the Baseline Security Policy described in chapter 1.3). If new vulnerabilities are detected in new Unify products or new versions of products which are still under development, the OBSO determines if the vulnerabilities may also impact already released products or versions and if customers using the released products or versions are at risk.
- Vulnerabilities reported by external security researchers and customers who conduct their own security audits. See chapter 3 for details.

[1] These sources include for example:

- Advisories from vendors (or open source SW providers) for components included in Unify products, such as suse.com, oracle.com, ibm.com opensuse.org, apache.org, kernel.org, openssl.org
- Advisories from governmental institutions and CERT organizations, such as us-cert.gov, cve.mitre.org, nvd.nist.gov
- Commercial vulnerability information provider

2.3. Assessment

2.3.1. Assessment of Vulnerability Information

Reported vulnerabilities are assessed by the OBSO for their relevance for Unify products. There is usually one of three possible results for each potentially affected product:

- **"False positive":**
  Although the vulnerability was initially assigned to a product, the assessment concludes that the product is not affected. Note that this is a very common case and covers the majority of reported vulnerabilities. It especially applies to vulnerabilities in Cat. 2 software components: Unify products usually only make use of a subset of the functions in a 3rd party component they have incorporated. The vulnerability often affects a part of that software that is not used, or the vulnerability is not exploitable in the context of the product.
  By default, the OBSO does not proactively inform customers about false positives.
- **"Configurative solution":**
  The vulnerability can be solved without a correction in the affected product.
  This is usually done by applying configuration changes on customer's systems or environment, in accordance with the relevant documentation (especially the product's Security Checklists and/or administration manuals).
  The OBSO decides on a case-by-case basis, if customers have to be informed through a Security Advisory. In most cases, this only applies, if the proposed configuration settings are not already documented in the above-mentioned manuals or if significant risk is seen for customer installations.
- **"Confirmed product security vulnerability":**
  The vulnerability is confirmed as a flaw in the product and needs a correction. The follow-up activities are aligned with the process as it applies to any software correction for the product in sustaining mode. Corrections for security vulnerabilities are prioritized according to the criteria described in the following chapter.
  Security Advisories are provided when significant risk is seen for customer installations.

2.3.2. Prioritization of Vulnerabilities

The following factors contribute to determining the urgency and prioritization of a correction for the vulnerability:

- "Original priority": what is the initial risk level or score given by the vendor of the affected software component or the reporter of the vulnerability?
- Is the vulnerability known to the general public (disclosed) or it is still undisclosed?
- What is the effort required to exploit the vulnerability – and are there already known exploits that impact the Unify's products?
- Are there effective countermeasures available that mitigate the risk?
- Is there more than one Unify product affected? If yes, is there a different risk level for each product?

The vulnerabilities are usually classified according to version 3.0[2] of the Common Vulnerability Scoring System (CVSS, see [3]).

Three different metrics are defined: Base, Temporal and Environmental and each metric calculates a score ranging from 0 to 10.

Based on past and current experience, vulnerabilities are classified inconsistently by different vendors. Therefore, CVSS is not used as the final score. Instead, the following simplifications are applied:

- Four risk levels are defined as priorities, ranging from 1 ("high") to 4 ("information only").
- In most cases, only the CVSS Base metric is used to determine the priority.
- In exceptional cases, the CVSS Temporal metric influences the priority (for example, if an existing vulnerability becomes known to be exploited "in the wild").
- As a rough guidance, the CVSS Base metric value of most vulnerabilities can be mapped as follows:

[2] Prior to July 2015, CVSS version 2.0 was used

Priority	Risk level	CVSSv3 Base metric
1	High	7.0-10.0 (High or Critical)
2	Medium	4.0-6.9 (Medium)
3	Low	0.1-3.9 (Low)
4	Information only	0.0 (None)

Figure 2 – Priorities and Risk Level of Vulnerabilities

2.4. Security Advisories (Customer Notification)

Security Advisories are issued by the OBSO and can be received by any interested customer or partner of Unify.
Customers and partners subscribed to the e-mail distribution list will receive an e-mail whenever a new Security Advisory is released or an existing Security Advisory is updated.

You can request to be added to (or removed from) the e-mail distribution list by using the contact address in chapter 3.4. (obso@atos.net).

Additionally, all Security Advisories that were released so far can be retrieved from the following public link [2]:

https://www.unify.com/security/advisories

The main purpose of the Security Advisory is for customers to determine if their assets need to be protected, to assess both the probability and impact of a threat and to decide on the appropriate countermeasures.

A Security Advisory contains the following information:

- **Description of the vulnerability:**
  Ideally, the description contains sufficient information (for customers to decide on the countermeasures), but not too detailed information (to prevent malicious attackers from creating and/or executing effective exploits)[3].
  The description also contains the results of the risk assessment (see chapter 2.3).
- **List of affected products:**
  The Unify products (incl. version numbers, if applicable) that are affected by the vulnerability are listed. This allows for immediate determination whether your individual solution might be at risk or not.
- **Recommended actions:**
  According to the definition in chapter 2.1.1, in most cases the OBSO recommends to apply the associated product update release or patch provided by Unify. Since more than one product or version may be affected by a single vulnerability, the advisory may also contain information about yet unpatched products or versions.
  If applicable, instructions for mitigation or configuration measures are given, how to mitigate or solve the vulnerability without having to apply the described software updates. The described configuration measures may address affected products as well as the customer's environment.
  In certain circumstances (for example if a particular vulnerability or security incident attracts high attention in the public, or if customers are explicitly asking for a statement), the OBSO may decide to release an advisory, even if no Unify product is affected. Usually, in those cases the recommendation will be: "nothing to do, but remain vigilant".
- **References:**
  A list of publicly accessible external links (URL) may be contained in the advisory. References are provided if the additional information helps customers to assess their risk and plan the countermeasures more accurately.[4]

[3] The amount and details of information is beyond the OBSO's influence for vulnerabilities of 3rd party components that are already publicly known.
[4] Although the OBSO makes every effort to ensure these links are accurate, up to date and relevant, we cannot take responsibility for external content.

3. Reporting and Feedback

Various forms of feedback and input regarding product security vulnerabilities can be sent to the OBSO, which is described in the next chapters. Contact details are given in chapter 3.4.

3.1. Report Product Security Vulnerabilities

Unify encourages customers, as well as independent security researchers or teams, to report potential vulnerabilities in Unify products.

The OBSO can be contacted directly, but customers are advised to report vulnerabilities via their established support channel in the same way as any other Unify product-related flaw.

Before contacting the OBSO, please

- Consider the definition of "product security vulnerability" in chapter 2.1.1
- Use the available product-related information – especially their Security Checklists and additional hardening information – to determine if the issue might be a "false positive" or can be solved without a correction in the affected product (see chapter 2.3.1 for more details)

When reporting a potential vulnerability in a Unify product, include as many details as possible, such as:

- The name and version of the product that may have the vulnerability, including the installed fix/hot fix releases and patches
- The type of the vulnerability (for example an SQL injection, cross-site scripting vulnerability, privilege escalation, buffer or integer overflow)
- Configuration settings that do (or may) impact the vulnerability and/or are relevant to reproduce the flaw
- Instructions how to reproduce the flaw (including what tools you have used)
- If available, your exploit code; alternatively, your estimation how the vulnerability could be exploited

In case the vulnerability is confirmed, a disclosure timeline will be agreed between the reporter and the OBSO. The agreement requires a case-by-case decision that depends on the severity of the vulnerability and the potential risk in typical customer installations, as well as the required effort to close the vulnerability and provide an update release or patch of the product.

If applicable and welcomed by the reporter, in Unify's sole discretion, credits are given in the associated Security Advisories.

3.2. Results of Security Audits

Customers who use our products as part of their solutions (both on-premise or as managed service) may perform IT Security Audits, Security Assessments or Penetration Tests at any time without having to ask the OBSO in advance.

Security Audits should be performed only after having applied all security configuration measures that are relevant according to the individual customer's security policy. Default recommendations are given in the hardening guidelines of every product, called Security Checklists. For other products involved in the audit, contact the vendor to retrieve similar information.

Typical recommendations contained in hardening guidelines are for example:

- All software is up-to-date and the latest security patches were applied
- Environmental systems, platforms or components (see Cat. 3 in chapter 2.1.2) are hardened according to the customer's guides. If there are no such guides, Unify recommends the use of the CIS Security Benchmarks (see [4])
- Unused services/ports are closed or disabled
- Individual strong passwords are set (according to the customer's password policy), and customer-specific digital certificates are installed (according to the customer's PKI policy)

- A state-of-the-art virus/malware protection solution is installed and running on all systems where it is considered relevant

Provided that these preconditions are met, the OBSO encourages customers to share the results of such security assessments with Unify.

Although similar assessments are already conducted during the development and test phases of all new products or product versions, no assessment can be exhaustive enough to serve as a single source to determine the security status of a system.

Instead of implementing customer-specific mitigations, any vulnerability reported by any customer helps to solve the issue in the affected Unify product(s) in a sustainable way. Therefore, every customer will benefit from the solution of the findings.

Customers are advised to provide security assessment reports via their established support channel. The report should only include findings that are suspect of being a “product security vulnerability” according to the definition in chapter 2.1.1.

Before reports submitted by a customer are processed further in the OBSO, they are anonymized appropriately to ensure that any existing non-disclosure agreements are not violated.

3.3. Feedback to Security Advisories

Any feedback regarding ambiguous description or errors contained in Security Advisories is welcome. Please contact your Service or Sales representative at Unify for clarification, consolidation and appropriate forwarding.

Note: OBSO cannot answer questions regarding the retrieval and the installation of associated product patches or fix releases mentioned in Security Advisories. Please follow the standard maintenance processes according to your individual service contract.

3.4. Contact Details

The OBSO can be contacted by sending an e-mail to: obso@atos.net

In case of confidential or sensitive information, please use S/MIME by requesting a signed unencrypted mail first, so you have our public key.

4. Security Services and Solutions in the Context of the VIP

The VIP contributes to a customer's individual information security management program.

Standardized procedures, for example according to ISO 27001 or the German BSI-100-2 (IT Grundschutzkatalog), will help to define, plan, implement and operate an Information Security Management program, that fits to the individual enterprise's needs.

Unify itself forcefully aligns its own Information Security Management with ISO 27001. Various Managed Services units have already been certified.

Furthermore, various customer solutions offered by Unify have already successfully implemented security measures according to the BSI standards 100-1,100-2, 100-3, and 100-4 as well as according to ISO 27001.

The definition and implementation of an Information Security Management system starts with an analysis to determine the essentially required security measures. Its implementation has certain degrees of freedom: some basic recommendations may be identified as impractical or unnecessary in the context of the overall security concept.

Unify will offer support in the alignment of your organization (or parts such as the communications management) to ISO 27001, as well as in the execution of a BSI Grundschutz analysis. Please contact your sales representative for more details.

5. References

[1] **Unify Product Lifecycle Policy**
https://www.unify.com/us/support/product-lifecycle-policy.aspx

[2] **Unify Product Security Advisories and Security Notes**
https://www.unify.com/security/advisories

[3] **CVSS (Common Vulnerability Scoring System) V3.0**
https://www.first.org/cvss

[4] **CIS (Center of Internet Security) – Security Benchmarks**
https://benchmarks.cisecurity.org

6. Glossary

BSI	Bundesamt für Sicherheit in der Informationstechnik (see: https://www.bsi.bund.de/EN/TheBSI/Functions/functions_node.html)
CERT	Computer Emergency Response Team
CIS	Center for Internet Security (see: https://cisecurity.org/)
CVSS	Common Vulnerability Scoring System (see: https://www.first.org/cvss)
EMSS	Extended Manufacturer Software Support
ISO	International Organization for Standardization (see: https://www.iso.org)
IT	Information Technology
OBSO	OpenScape Baseline Security Office
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
SBC	Session Border Controller
SQL	Structured Query Language
SW	Software
UC	Unified Communications
URL	Uniform Resource Locator
VIP	Vulnerability Intelligence Process

About Unify

Unify is the Atos brand for communication and collaboration solutions. At the core of the Atos Digital Workplace portfolio, Unify technology enables organizations of all sizes to transform the way they collaborate, creating a more connected and productive workforce which can dramatically improve team performance, individual engagement and business efficiency.

Unify products represent a strong heritage of technology innovation, reliability and flexibility. Their award-winning intuitive user experience can be delivered through almost any device and in any combination of cloud or on-premise deployment. Augmented by Atos' secure digital platforms, vertical solutions and transformation services, they set the global standard for a rich and reliable collaboration experience that empowers teams to deliver extraordinary results.

unify.com

unify
atos collaboration solutions