

Public



SECURITY POLICY - VULNERABILITY INTELLIGENCE PROCESS

AUTHOR(S)	: OpenScape Baseline Security Office
DOCUMENT NUMBER	: UFM-PLM-0009
VERSION	: 1.6
STATUS	: Released
SOURCE	: Unify
DOCUMENT DATE	: 30 October 2023
NUMBER OF PAGES	: 22

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks Corporation (MITEL®)**. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC), its affiliates, parents, or subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

®,™ Trademark of Mitel Networks Corporation

© Copyright 2023, Mitel Networks Corporation

All rights reserved

Contents

- 1 Introduction7
- 1.1 Purpose7
- 1.2 Applicability and Scope7
- 2 Baseline Security Policy8
- 3 Vulnerability Intelligence Process (VIP)9
- 3.1 Definition of “Product Security Vulnerability”9
- 3.2 Scope of the VIP9
- 3.3 Active Monitoring 11
- 3.4 Assessment of Vulnerability Information 11
- 3.5 Prioritization of Vulnerabilities 12
- 3.6 Security Advisories (Customer Notification) 13
- 3.7 Fixed Security Vulnerabilities 16
- 3.8 How Partners and Customers can access release notes 16
- 4 Reporting and Feedback 18
- 4.1 Reporting of Product Security Vulnerabilities by Security Researchers 18
- 4.2 Customer Reported Security Vulnerabilities 18
- 4.3 Feedback to Security Advisories 19
- 4.4 Contact Details 19
- 5 Unify Cloud Services 21
- 5.1 Unify Cloud Client Applications 21
- 5.2 General Provisions for Unify Cloud Services 21
- 6 References 22

List of changes

version	Date	Description
1.0	27th June 2012	Initial draft.
1.1	11th Nov 2013	Update release (company rebrand, organisational changes)
1.2	1st Feb 2016	Chapter 1.4: updated product list; added reference to Atos 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 Atos Unify Security Advisories Chapter 3.4: updated PGP encryption key Various editorial changes
1.2.1	23rd May 2018	Update Logo, remove PGP
1.2.2	3rd April 2019	Replace obso@unify.com with obso@atos.net
1.2.3	3rd June 2019	Add document number
1.3	30th Sep 2019	Chapter 1.3: Included hardening scripts Chapter 1.4: Updated product scope Chapter 3.1: Revision of reporting security vulnerabilities Deleted chapter 4 on Security Solutions and Services Minor text updates in several chapters
1.4	3rd July 2020	Chapter 1.2: Added OpenScape First Response Chapter 2: Baseline Security (added General Security Requirements, Vulnerability Scanning) Rebranding of document based on Atos policy template
1.5	7 th November 2022	Chapter 1.2: Deleted OpenScape Enterprise Express and OpenStage phones / added Virtual Care Collaboration Service and Unify Phone. Chapter 3.5: added critical risk category Chapter 3.6: changed procedures for information about advisories / introduction of TLP for classified content Chapter 4.3: Minor updates Chapter 5: Updated references
1.6	30 th October 2023	Terms and abbreviations Chapter 1.2: Updated Applicability and Scope Chapter 3.6: Updated TLP descriptions Chapter 3.7 (New): Fixed Security Vulnerabilities Chapter 3.8 (New): How Partners and Customers can access release notes Chapter 5 (New): Unify Cloud Services

Target readers, communication method

Target group	Distribution / publication method
All Unify employees	Published on Unify Integrated Management System
Customers and Partners	Published on Unify Security Advisories website

Terms and abbreviations

Terms / Abbreviations	Description
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://ciscure.org/)
CVSS	Common Vulnerability Scoring System (see: https://www.first.org/cvss)
ISO	International Organization for Standardization (see: https://www.iso.org)
IT	Information Technology
OBSO	OpenScape Baseline Security Office
Policy	In a policy, an organization formally states a system of principles of behavior, conduct etc. thought to be desirable or necessary, to avoid some negative effect, or to seek some positive benefit.
Procedure	Procedures are set of actions that is the official or accepted way of doing something.
Process	Processes describe the lower-level approach, including inputs & outputs, workflow, roles and responsibilities, sequence and interaction, determine and apply the criteria and methods (including monitoring, measurements and related performance indicators) needed to ensure the effective operation and control of these processes, resources, assign the responsibilities and authorities, address the risks and opportunities, evaluate these processes and implement any changes needed to ensure that these processes achieve their intended results, improve the processes and the quality management system.
PSA	Practical Security Assessment
SBC	Session Border Controller
SQL	Structured Query Language
TSA	Theoretical Security Assessment
UC	Unified Communications
URL	Uniform Resource Locator
VIP	Vulnerability Intelligence Process

1 Introduction

1.1 Purpose

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 an Unify product was released.

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

It regulates how to

- Identify, analyze and resolve security vulnerabilities in released Unify products, and
- Deliver guidance to customers how to mitigate or close these vulnerabilities.

1.2 Applicability and Scope

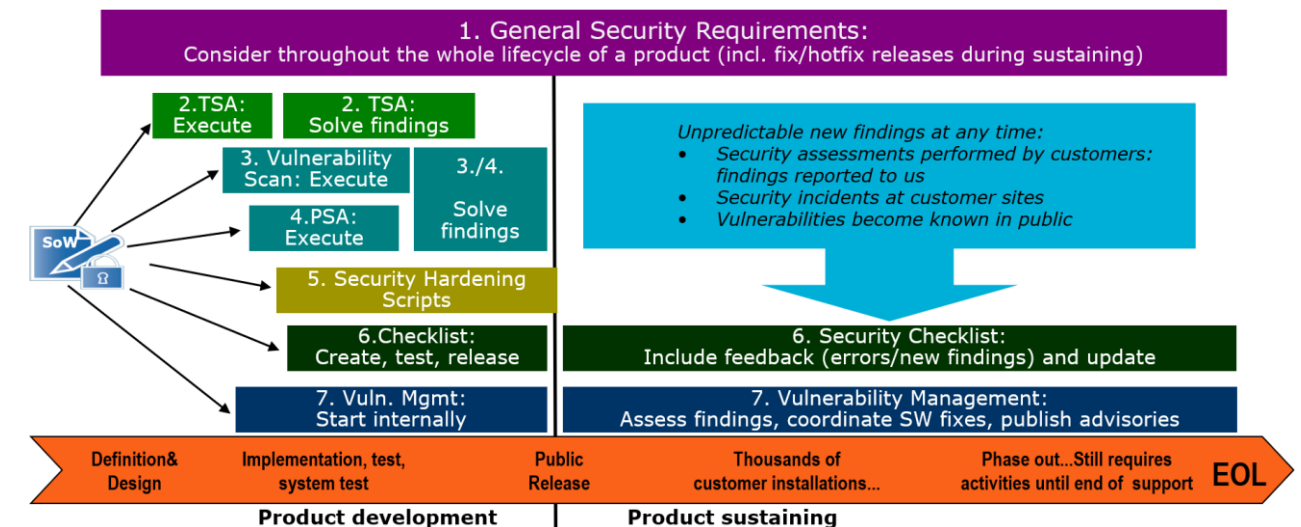
In the current version, the process applies to the following Unify OpenScape product areas provided by Unify:

- Voice platforms including gateways (such as OpenScape Voice/Branch/SBC, OpenScape 4000, OpenScape Business)
- Circuit Nodes, Circuit Telephony Connector, Circuit Integrations (e.g. Circuit for Outlook..)
- 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, Composer)
- End-user devices and applications (such as OpenScape Desk Phone CP phones, OpenScape UC desktop applications and mobile apps, Circuit apps)
- OpenScape Contact Center
- OpenScape Xpert
- OpenScape Alarm Response
- OpenScape License Management
- Virtual Care Collaboration Service
- Unify Phone for Unify Video and Unify Phone for OpenScape

All products that belong to these areas are actively monitored for potential vulnerabilities, from the first day they have been released to GA (General Availability), until their End of Standard Support (M44). Extended Manufacturer Software Support is covered in the Unify Product Lifecycle Policy.

2 Baseline Security Policy

The Security Policy - Vulnerability Intelligence Process (VIP) is an integral part of the Baseline Security Policy at Unify. In addition to the 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 definition and design:

- Evaluation of products against **General Security Requirements**
- Threat and risk analysis (**Theoretical Security Assessment**) to determine the essential security requirements for the product

Product development and testing:

- **Vulnerability Scanning** identifies known weaknesses in systems and applications.
- 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 and Hardening Scripts**) to support the configuration and hardening 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

3 Vulnerability Intelligence Process (VIP)

The VIP is within the responsibility of the OpenScope 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 3.2. The following chapters describe the key elements of the VIP in detail:

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

3.1 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 “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.

3.2 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 3.6) which they are able to consider in their own vulnerability assessment and patch processes.

A security vulnerability is usually 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 connect to)

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.

For **Cat. 2 vulnerabilities** to belong to the VIP it depends on the individual 3rd-party software component 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.

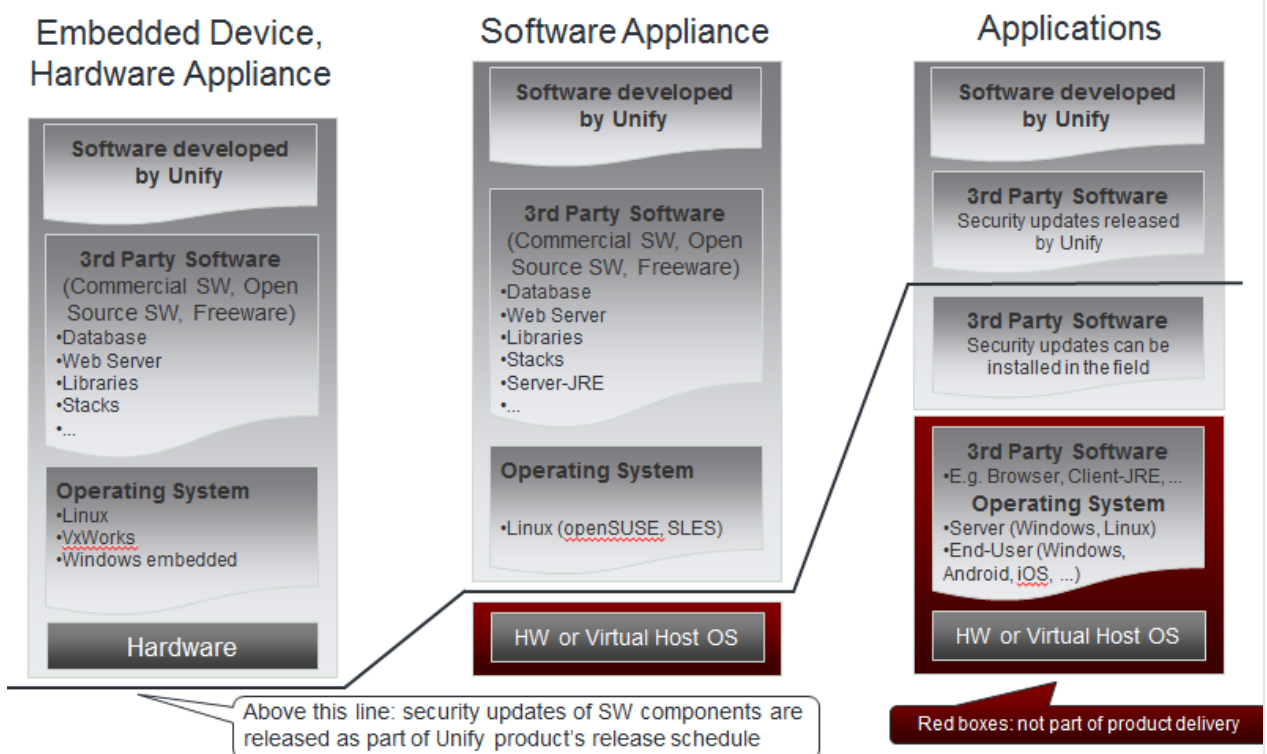


Figure 1 – Product types and applicability of security updates

3.3 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 providers¹. 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 2). 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 4 for details.

3.4 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-

¹ These sources include for example:

- Advisories from vendors (or open source Softwareproviders) 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

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.

3.5 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?
- What is the effort required to exploit the vulnerability – and are there already known exploits that impact 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 3.1² 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:

- Five risk levels are defined as priorities, ranging from 1 (“critical”) to 5 (“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:

Priority	Risk level	CVSSv3 Base metric
1	Critical	9.0-10.0 (Critical)
2	High	7.0-8.9 (High)
3	Medium	4.0-6.9 (Medium)
4	Low	0.1-3.9 (Low)
5	Information only	0.0 (None)

Figure 2 – Priorities and Risk Level of Vulnerabilities

² Prior to July 2015, CVSS version 2.0 was used

3.6 Security Advisories (Customer Notification)

Security Advisories are issued by the OBSO. Upon General Release a Security Advisory is published on the Unify website on the following public link [2]:

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

Unify may decide to issue statements about Security Vulnerabilities before the General Release of a Security Advisory as a Knowledge Base Article within the Unify ServiceNow Portal [5]. Security Advisories and Knowledge Base Articles before General Release are classified according to the Traffic Light Protocol (TLP) [6] and must be treated according to their classification.






Color	When should it be used	How may it be shared
 <p>TLP: Red Not for disclosure, restricted to participants only.</p>	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
 <p>TLP: Amber+Strict Limited disclosure, restricted to participants' organization.</p>	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
 <p>TLP: Amber Limited disclosure, restricted to participants' organization and its clients (see Terminology Definitions).</p>	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
 <p>TLP: Green Limited disclosure, restricted to the community.</p>	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
 <p>TLP: Clear Disclosure is not limited.</p>	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

Figure - TLP definitions (source: <https://www.cisa.gov/tlp>)

Customers and partners may subscribe to the Security Advisory distributions list . Subscribers to the e-mail distribution list will receive an e-mail whenever a new Security Advisory has been released. You can request to be added to (or removed from) the e-mail distribution list by sending a message using the contact address 4.4 obso@atos.net.

Information about Security Advisories will also be distributed via Twitter/X. [Follow @UnifyCoSecurity](#) on Twitter/X or search for [#obso](#):
<https://twitter.com/unifycosecurity>

Information on updates for Security Advisories upon General Release will be provided on the public website. In addition, a short Tweet will be provided about the Security Advisory that has been updated.

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:**
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 3.4).
- **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 3.1, in most cases the OBSO recommends applying 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.

- **Versions Change History:**
It contains a brief description of the changes that have been done for a particular version and the publication date of the version.

3.7 Fixed Security Vulnerabilities

Vulnerabilities that are identified as part of the Unify vulnerability management process may be updated as part of any software release (major, minor, fix release, hotfix). The information about vulnerabilities that have been fixed is regularly included in the release notes for the corresponding product. Hence, it is recommended to frequently check the Release Notes and frequently update software to the most current releases.

The release notes include a section **Resolved Vulnerabilities;**

2.3 Resolved Vulnerabilities

(if nothing please insert "Not applicable for this release")

Tracking Reference	Internal Reference	Severity Level	Summary	Released in Version
[e.g., ticket or CVE number, security advisory ID]	[e.g., Jira ID]	[Critical/High/Medium/Low (Mandatory), CVSS 3.1 <u>Score</u> (Optional)]	[high level summary statement only, detailed description must not be included]	

Note: It is strongly recommended applying the fix version if it includes resolved vulnerabilities.

3.8 How Partners and Customers can access release notes

If you are a Partner you have access to the Release Notes via the Partner Portal.

As a registered Customer you may access the Release Notes via the Atos Web Support Portal.

Customers and partners can send account requests to the following functional mail boxes.

Customers:

ccs_support_portal@atos.net

Partners:

UCC.IT-servicedesk@atos.net

Information about Release Notes is available within the Product Information Database (PIM). Access to the PIM from the Atos Web Support Portal (AWSP) is available through the AWSP more applications (see KB000105101). Within the PIM information about Software Releases and Hotfixes is available in the Service Info & Hotfixes section.

As a registered Customer you may access the Release Notes via the Atos Unify Web Support Portal.

Customers and partners can send account requests to the following functional mail boxes.

Customers:

ccs_support_portal@atos.net

Partners:

UCC.IT-servicedesk@atos.net

Information about Release Notes is available within the Product Information Database (PIM). Access to the PIM from the Atos Web Support Portal (AWSP) is available through the AWSP more applications (see KB000105101). Within the PIM information about Software Releases and Hotfixes is available in the Service Info & Hotfixes section.

4 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 4.4.

Before contacting the Unify Support or the OBSO, please

- Consider whether the software version that you run is up to date. Testing for security vulnerabilities should always target the latest software versions provided
- Evaluate whether the issue is considered a “product security vulnerability” according to the definition in chapter 3.1.
- 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 3.4 for more details)
- Information provided must be provided in English

4.1 Reporting of Product Security Vulnerabilities by Security Researchers

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

When reporting a potential vulnerability in an 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)
- Scanning results/assessment reports with a description of the vulnerability identified
- 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.

4.2 Customer Reported Security Vulnerabilities

We differentiate between customer penetration tests that are customer initiated and that identify vulnerabilities within the code of the Unify software and vulnerability scans.

The results of customer-initiated penetration tests may be submitted through the OBSO and will follow the same procedure as described in chapter 4.1.

Handling of vulnerabilities identified in vulnerability scans:

Customers shall report single product specific vulnerabilities via their established support channel. The issue will be reported as a problem.

When reporting a potential vulnerability in an Unify product the following information needs to be included:

- 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)
- Scanning results/assessment reports with a description of the vulnerability identified

Upon reporting the vulnerability, customers may request the following information:

- Information whether the product is affected by the vulnerability.
- Information about the fix plan including a timeline.

Whether a vulnerability is fixed is in the sole discretion of Unify.

If a fix is planned:

- An internal ticket number is opened and provided for reference of the planned improvement.
- The problem ticket will be closed.

Fixed vulnerabilities are published in release notes of the respective products with the internal ticket numbers included as a reference.

4.3 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: The 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 and support processes according to your individual service contract.

4.4 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.

5 Unify Cloud Services

Unify Cloud Services relates to a set of services provided as Software-as-a-Service to our customers and partners that are developed, implemented and managed by Unify. The part that is fully managed by Unify is usually referred to as the Backend of the Cloud Services. Access to the cloud services may be either through a web browser or client applications provided by Unify that a customer may have to install in order to get access to the cloud services.

5.1 Unify Cloud Client Applications

The vulnerability management for Unify Cloud Client Applications that provide access to the Unify Cloud Services is not any different from on-premise systems and applications. All the provisions described in chapters 2-4 apply.

The scope of Unify Cloud Client Applications includes:

- Unify Phone mobile clients for iOS and Android
- Unify Phone Chrome extension

5.2 General Provisions for Unify Cloud Services

The scope of Unify Cloud Services includes:

- Unify Phone Backend including the Unify Phone Web Client
- Unify Phone Tenant Administration

The security measures defined within the Unify Secure Development Lifecycle and governed by the Unify Baseline Security Policy in Chapter 2 fully apply to the Unify Cloud Services.

The vulnerability management procedures as described in Chapter 3 do only partially apply to cloud services:

- Chapters 3.1, 3.3, and 3.4 fully apply for the Unify Cloud Services as well and vulnerabilities are continuously evaluated and remediation considering Unify policies, the risk and availability of fixes for the vulnerabilities identified.
- Chapter 3.2 is not relevant for the cloud services as Unify is fully responsible for the vulnerability management.
- Chapter 3.6-3.8 are not relevant for Unify cloud services in the context of vulnerability management as Unify does not publish fixed vulnerabilities in the Release Notes or Security Advisories.

The reporting of vulnerabilities follows the same procedures as described in Chapter 4.

6 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) V3.1**
<https://www.first.org/cvss>
- [4] **CIS (Center of Internet Security) – Security Benchmarks**
<https://benchmarks.cisecurity.org>
- [5] **Atos ServiceNow Portal**
<https://atosunify.service-now.com/unify>
- [6] **TLP (Traffic Light Protocol)**
<https://www.cisa.gov/tlp>