Unify OpenScape 4000 Platform V11(System and Manager)

Release Notes

Software Version: V11 R0.22.1

2024-06-27

☐ Major Release ☐ Minor Release ☐ Fix Release ☒ Hotfix Release

Current release status can be verified via the Software Supply Server (SWS)

Deliverables

☐ Full Release ☒ Delta Release

Export Control Classification Data

AL: 5D002C1A ECCN: 5D002ENCR

Release Notes Version: V1.0

About this document

This document provides general information about the release, generics, and other relevant notes for the corresponding product and its correction versions.

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. 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.

Unify OpenScape 4000 Platform
2024-06-27

Delivered Files

Product Item Number		File Name
1	P30152-P1698-H1-1	PLT-V11_R0.22.1.tar
2		
3		

Table of Contents

1. History of Change

1.1. Release Notes content

Version	Date	Description of changes
1.0	2024-06-27	Initial creation for V11 R0.22.1

1.2. Product versions history

Software Version	Production Version	Date	Remarks
V11 R0.22.1	V11 R0.22.1 PLT HF	2024-06-27	

2. Changes

2.1. Implemented Change Requests / New features

Tracking Reference	Internal Reference	Summary	Released in Version
	OSFOURK-26572	Installation of OSEM on standard EcoServer SSD	V11 R0.22.1
	OSFOURK-27015	Add static routes in RKE2 for licensing	V11 R0.22.1
	OSFOURK-27392	DTB: Start dialling number from search list with green handset button (DECT device); Remark: requires new CMI LW (CVx158)	V11 R0.22.1
	OSFOURK-27376	DTB: Enable green button to make the call directly when a contact is selected from Common/Private directory or Journal Call; Remark: requires new CMI LW (CVx158)	V11 R0.22.1

2.2. Resolved Reported Problems / Symptoms

Tracking Reference	Internal Reference	Summary	Released in Version
		For details see attached “RN_OS4K_PLT-HF_V11-R0_22_1” from Nuxeo.	

2.3. Resolved Vulnerabilities

Tracking Reference	Internal Reference	Severity Level	Summary	Released in Version
PRB000076483	OSFOURK-27447	Critical, CVSS 9.8	An OS command injection vulnerability that may allow an unauthenticated attacker to upload arbitrary files and get administrative access to the system. [1)]	V11 R0.22.1
PRB000076495	OSFOURK-27449	Critical, CVSS 9.8	An OS command injection vulnerability that may allow an unauthenticated attacker to upload arbitrary files and get administrative access to the system. [1)]	V11 R0.22.1
PRB000076530	OSFOURK-27463	Critical, CVSS 9.8	An OS command injection vulnerability that may allow an unauthenticated attacker to upload arbitrary files and get administrative access to the system. [1)]	V11 R0.22.1
PRB000076605	OSFOURK-27480	Critical, CVSS 9.8	An OS command injection vulnerability that may allow an unauthenticated attacker to upload arbitrary files and get administrative access to the system. [1)]	V11 R0.22.1
CVE-2018-6798	OSFOURK-27490	Important, CVSS 7.5	Matching a crafted locale dependent regular expression can cause a heap-based buffer over-read in Perl	V11 R0.22.1
CVE-2023-5676, CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-20926, CVE-2024-20945, CVE-2024-20952	OSFOURK-26992	important, CVSS 4.7 - 7.4	SUSE Enterprise Linux Security Update for java-1_8_0-openj9 (SUSE-SU-2024:0479-1)	V11 R0.22.1

1) We'd like to thank DB Systel for disclosing and supporting us to remediate the issue

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

3. Important Issues, Workarounds, Hints and Restrictions

This section provides the latest information at time of software release and is only pertaining to the time of release notes generation.

3.1. Important Issues

Tracking Reference	Internal Reference	Summary	Workaround / Actions
	OSFOURK-26572	OSEM on standard EcoServer SSD	See description in chapter 4.2
	OSFOURK-27619	no Kubernetes menu in Portal after recovery script Recovery script is setting the 4kube status to disabled in haipsetup.xml, but OSEM keeps running.	The situation can be corrected by executing the following command on the Linux Platform: /opt/yapp/writehaipxml.sh system.has4Kube=1
	OSFOURK-27588	OSEM - 404 error after installation Sporadically, after deploying OSEM, its homepage fails to load.	In 4kube shell, execute the following command, or ask for GVS instructions: kubectl apply -f metallb-ip-pool.yaml

3.2. Workarounds, Hints

Not applicable for this release

Tracking Reference	Internal Reference	Summary	Workaround / Actions

3.3. Restrictions

Not applicable for this release

Tracking Reference	Internal Reference	Summary	Workaround / Actions

4. Installation and Upgrade / Update

4.1. Installation

Platform Hotfixes are released for activation on OpenScape 4000 System and Manager Appliances.

4.2. Upgrade / Update / Migration

The precondition for the activation of a PLT-Hotfix is the V11 R0.22.0 .

The hotfix is transferred by means of SWM and activated using SWA.

<u>**Expected telephony downtime on VoIP Gateways**</u>

Activating Platform Hotfix V11 R0.22.1 will cause a short telephony downtime on all SoftGates, Enterprise Gateways and STMIX boards at the moment it is activated (via SWA on central host, via APE HBR on Survivable SG/EntGW platforms, via Gateway Manager on STMIX and Standalone SG/EntGW), due to the restart of the SoftGate Application.

Reason: Update of the Java JRE due to Security Vulnerabilities (CVE-2023-5676, CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-20926, CVE-2024-20945, CVE-2024-20952, ...), requires a restart of all Java based processes.

On the central host itself, there will be no telephony downtime when activating the platform Hotfix in Assistant “Software Activation” / “Software-Aktivierung.

Exception: Integrated SoftGates on central hosts (Simplex deployment only) or on Quorums of separated Duplex deployments will be restarted automatically during platform hotfix activation in SWA.

OSFOURK-26572 Installation of OSEM on standard EcoServer SSD

If OSEM is not present on the system, we recommend using PLT Hotfix V11 R0.22.1 as a base for the OSEM deployment.

For Ecoserver2/Branch2 systems, all features based on SoftRAID (=using two disks in RAID, creating Recovery Disk) will work also with OSEM enabled and related data.

After Hotfix V11 R0.22.1 is applied, the OSEM can be activated on all OS4K certified SSDs (this includes 240GB SSDs).

Note: Potentially 1 TB SSDs can be used further on, there is no need to replace them.

For VM Simplex/Survivable, Platform Portal will check the existing RAM Memory, and ask for extra 2GB over the OVF default 8GB, before allowing Kubernetes and OSEM to be enabled.

Standalone softgate VM also needs extra 2GB RAM Memory, over the OVF default 4GB.

If OSEM is already present on the system, PLT Hotfix V11 R0.22.1 can be safely activated.

For Ecoserver2/Branch2 systems, after PLT Hotfix V11 R0.22.1 activation, if the above features will be needed, OSEM must be re-deployed: we strongly recommend saving OSEM configuration data, then disabling Kubernetes (via Platform Portal -> System -> LAN Configuration -> Disable integrated Kubernetes), then re-enable integrated Kubernetes, re-deploy OSEM and restore its configuration.

For VM Simplex/Survivable, after PLT Hotfix V11 R0.22.1 is activated, there is no need to redeploy OSEM. Assistant Dashboard will warn about the need for extra 2GB RAM Memory on VM, for safely keep running OSEM.

Standalone softgate VM also needs extra 2GB RAM Memory, over the OVF default 4GB.

OSFOURK-27015 add static routes in RKE2 for licensing

The fix enables the using of online licensing for OSEM.

Important Note: Activation of Platform-Hotfixes should not be made directly on APE Nodes!!!

Software updates should be activated directly on the Host system and will be mirrored to the APE nodes during the next APE restore process (i.e. through automatically scheduled or manual APE Backups).

4.2.1. Fallback

Not possible

4.3. Special settings and instructions

Not applicable for this release

5. Hardware and Software Compatibility

5.1. Hardware

Not applicable for this release

5.2. Firmware

Not applicable for this release

5.3. Loadware

Not applicable for this release

5.4. Software / Applications

Not applicable for this release

5.5. Operating systems

Operating System Name	Operating System Version
Linux	Based on openSUSE Leap15.5

DO NOT MAKE ANY LINUX UPDATES.

SECURITY PATCHES AND OTHER SOFTWARE UPDATES WILL BE DELIVERED IN OPENSCAPE 4000 RELEASES.

DO NOT INSTALL ANY OTHER SOFTWARE.

5.6. Compliant products

This section lists the versions associated with the communication platforms, other products and third-party products that have been tested for use with this version of the product and are known to work.

5.6.1. Communication platforms

Hardware and software products that have been tested together with this version of the product are listed in the common compatibility matrix, which also includes the respective versions required to use with the current version of this product.

The current Common Compatibility Matrix can be found on the Unify Partner Portal https://unify.com/en/partners/partner-portal under Sell - Portfolio Information.

Note: Use the "Search & Find" option under Portfolio Information and Search Documentation for "Common Compatibility Matrix" (search on title only!).

5.6.2. Other products

Not applicable for this release

5.6.3. Third-Party products

Not applicable for this release

6. Service Information

6.1. Product tooling structure

Main Category	Communication Systems
Product Family	OpenScape 4000
Product	OpenScape 4000
Product Version	OpenScape 4000 V11
Product Item Number	P30152-P1698-H1-1 (V11 R0.22.1)

6.2. Case tracking system

Tickets can be generated and tracked via the WEB Support Portal (AWSP).

http://atosunify.service-now.com/unify

A short instruction can be found on the AWSP directly.

7. Documentation Reference

The product documentation can be found on the Unify Partner Portal https://unify.com/en/partners/partner-portal under Sell - Portfolio Information.

8. References

Not applicable for this release