



DGW Firmware

V50.0.3127

Security Improvement Notes

Security Improvement Notes

DGW Application 50.0.3127

- [Summary](#)
- [Security Changes](#)

Summary

ID	Synopsis
DGW-17040	The VNC server used by the VM service can now be automatically disabled after a configurable period
DGW-17218	Upgrade Dropbear SSH server to version 2025.88
DGW-17219	Upgrade wpa_supplicant client to version 2.11
DGW-17288	Upgrade to OpenSSL 3.5.0
DGW-17351	New parameters added to the Dcm.PasswordEncryption table
DGW-17356	Support RFC8760 (SIP auth SHA256) for SIP client authentication
DGW-17395	Web service does not send complete certificate chain in TLS handshake

Security Changes

DGW-17395 - Web service does not send complete certificate chain in TLS handshake

Incident Number: ID-10433

Fixed an issue where the Web service would not send the complete certificate chain during the TLS handshake.

DGW-17356 - Support RFC8760 (SIP auth SHA256) for SIP client authentication

The SipEp service now supports RFC 8760 authentication. Supported algorithms are:

- MD5
- MD5-sess
- SHA-256
- SHA-256-sess
- SHA-512-256
- SHA-512-256-sess

DGW-17351 - New parameters added to the Dcm.PasswordEncryption table

The following parameters were added to the Dcm.PasswordEncryption table:

- Conf.ScriptsTransferPassword
- Conf.ScriptsSecretKey
- Conf.ScriptExportSecretKey
- Conf.ImageTransferPassword
- Conf.ImageSecretKey
- Cwmp.Password
- Cwmp.ConnectionRequestPassword
- Fpu.MfpTransferPassword
- Moh.Password
- Snmp.PrivPassword
- Snmp.SnmpV3Password

Note: Moh.Password and Snmp.PrivPassword now have a maximum length of 63. Passwords with a length greater than 63 will be lost when upgrading.

DGW-17288 - Upgrade to OpenSSL 3.5.0

The application was re-built using OpenSSL 3.5.0.

The DGW application now prioritizes tls1.3 over tls1.2 when both versions are supported.

DGW-17219 - Upgrade wpa_supplicant client to version 2.11

The application was re-built using wpa_supplicant client version 2.11.

DGW-17218 - Upgrade Dropbear SSH server to version 2025.88

The application was re-built using Dropbear SSH server version 2025.88.

DGW-17040 - The VNC server used by the VM service can now be automatically disabled after a configurable period

Incident Number: ID-9791

Two new settings allowing to automatically disable the VNC server after a certain delay have been added.

When the feature is enabled (**Vnc.AutomaticVncShutdownEnable**), a VM's VNC ID (**Vm.Vm.VncDisplayId**) will automatically be set to -1 (**disabled**) upon expiration of the specified timer (**Vm.AutomaticVncShutdownTimer**), starting from the virtual machine startup.



Copyright Notice

Copyright © 2025 Media5 Corporation.

This document contains information that is proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.



130, rue Sauvé
Sherbrooke (Québec)
J1L 0A7 Canada
media5corp.com