

Qubes OS Functionality (Selective Screenshots)

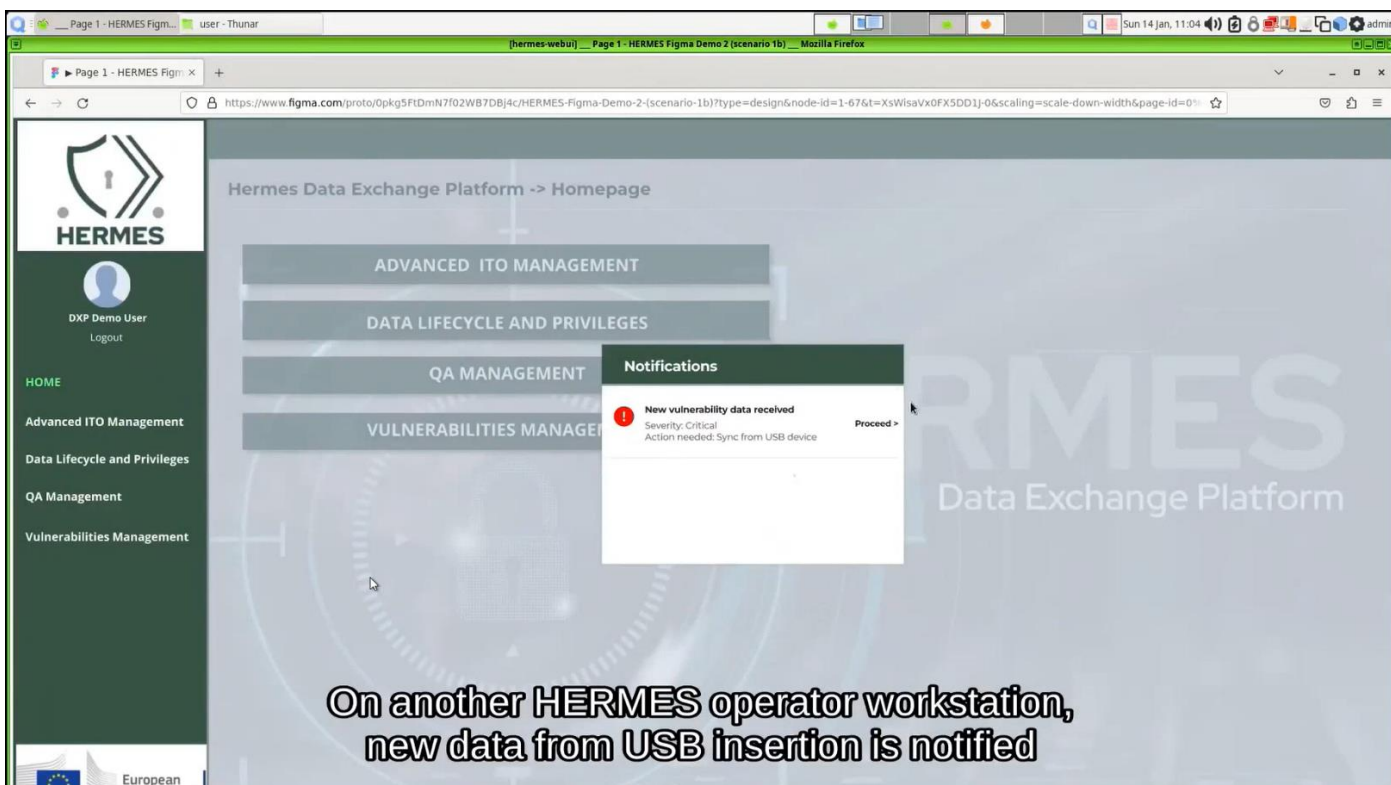
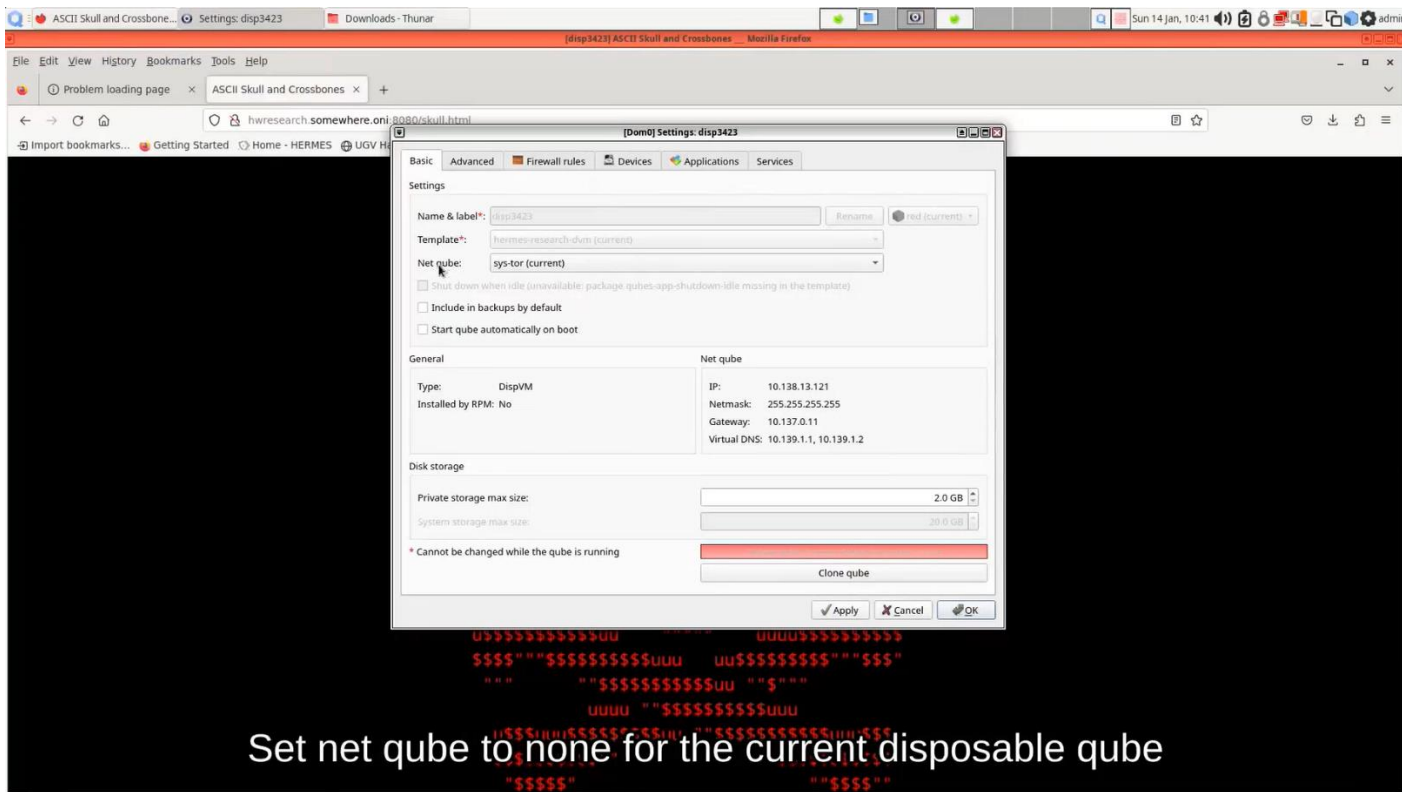
The screenshot shows the Qube Manager interface on the left, displaying a list of running VMs. The 'sys-firewall' VM is highlighted. On the right, a network diagram illustrates the connectivity between various services. The diagram shows a central 'sys-firewall' connected to 'sys-net' (WAN), 'sys-tor', and 'vpn-pltf'. 'sys-tor' is connected to 'disp8901' and 'disp4567'. 'vpn-pltf' is connected to 'hermes-webui' and 'vpn-hq'. 'hermes-webui' is connected to 'hermes-notification'. 'hermes-notification' is connected to 'hermes-exchange'. 'hermes-exchange' is connected to 'hermes-exchange-usb' and 'hermes-inbox'. 'hermes-exchange-usb' is connected to 'sys-usb'. 'hermes-inbox' is connected to 'disp0123' and 'disp4567'. The diagram also shows 'RPC - HERMES' connections between 'hermes-exchange' and 'hermes-inbox', and 'RPC - Copy' connections between 'hermes-inbox' and 'disp0123'.

hermes-webui: access HERMES platform

The screenshot shows a web browser displaying a page titled "UGV Hardware Vulnerabilities". The page lists four vulnerabilities:

- Vulnerability 1: CVE-2023-UGV-12345**
CVE-2023-UGV-12345 is a critical vulnerability in the XYZ Hardware, an UGV hardware device. This vulnerability allows remote attackers to execute arbitrary code and gain unauthorized access to the device. It affects all versions of the XYZ Hardware prior to version 3.0. Users are strongly advised to update to the latest version immediately.
- Vulnerability 2: CVE-2023-UGV-67890**
CVE-2023-UGV-67890 is a high-severity vulnerability found in the UGV-FW-Delta-2023 Hardware. Attackers with physical access to the device can exploit this vulnerability to bypass authentication and gain control of the device. The vendor has released a security patch for affected devices, and users are encouraged to apply the update as soon as possible.
- Vulnerability 3: CVE-2023-UGV-54321**
CVE-2023-UGV-54321 is a moderate-level vulnerability affecting the LMN Hardware. This vulnerability allows attackers to conduct denial of service attacks by sending specially crafted packets to the device. The vendor is aware of the issue and is working on a fix, which is expected to be released in the next software update.
- Vulnerability 4: CVE-2024-UGV-88888**
CVE-2024-UGV-88888 is a low-severity vulnerability that affects the PQR Hardware. Please note that the above vulnerabilities and hardware devices are entirely fictional and are provided for illustrative purposes only.

Conduct security research within the disposable qube



HERMES

DXP Demo User
Logout

Home
Advanced ITO Management
Data Lifecycle and Privileges
QA Management
Vulnerabilities Management

European Commission
This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101019719. HERMES: This design reflects only the author's view. The European Commission is not responsible for any use that may be made of the information it contains.

List of UGV's Firmwares

List of Vulnerabilities

VULNERABILITY NAME	FIRMWARE NAME	VULNERABILITY DESCRIPTION	SEVERITY	REPORTED UPDATE
CVE-2022-UGV-001	UGV-FW-Alpha-2022	Unsecured command and control interface in UGV Management System allows remote attackers to execute arbitrary commands, compromising vehicle control.	High	10 Jan 2024
CVE-2023-UGV-002	UGV-FW-Beta-2022	Buffer overflow vulnerability in UGV sensor processing module permits attacker to execute malicious code through specially crafted sensor data, leading to unauthorised access.	Critical	09 Jan 2024
CVE-2023-UGV-003	UGV-FW-Gamma-2023	UGV communication encryption weakness exposes sensitive data during transmission, enabling attackers to eavesdrop on communication between the vehicle and control center.	Medium	1 Jan 2024
CVE-2024-UGV-004	UGV-FW-Delta-2023	Cross-site scripting (XSS) in UGV telemetry web interface allows attackers to inject malicious scripts, potentially leading to unauthorised access or data theft.	High	1 Aug 2023
CVE-2025-UGV-005	UGV-FW-Epsilon-2024	Denial-of-service (DoS) vulnerability in UGV navigation system allows remote attackers to disrupt vehicle navigation by sending specially crafted data packets, causing a service outage.	Moderate	10 Jun 2023
CVE-2023-UGV-67890	UGV-FW-Delta-2023	CVE-2023-UGV-67890 is a high severity vulnerability found in the UGV-FW-Delta hardware. Attackers with physical access to the device can exploit this vulnerability to bypass authentication and gain control of the device.	Critical	19 Jan 2024

ADD VULNERABILITY
LOAD VULNERABILITY
SYNC TO USB
SYNC FROM USB

Notify Op. Center

On the dedicated qube for notifying operation center of the critical vulnerability

Qube Manager

[Dom0] Qube Manager

System Qube View About

New qube Delete qube Start/Resume Emergency pause Shutdown Restart Settings Edit firewall App shortcuts Update

Search: Show: Running Halted Network Templates Standalone All

Name	Template	Net/VM	Disk Usage	Internal	Backup	Last backup
dom0	Admin/VM	n/a	n/a			
PKI	hermes-base	ER	0.0 MiB			
HAPI	hermes-base	EG	0.0 MiB			
HDM	hermes-base	EG	0.0 MiB			
HDS	hermes-base	EG	0.0 MiB			
HDX	hermes-base	EG	0.0 MiB			
HUI	hermes-base	EG	0.0 MiB			
ER	hermes-base	EG	33.79 MiB			
sys-net	fedora-39-xfce	n/a	1121.28 MiB			
sys-usb	default-dvm	n/a	0.0 MiB			
EG	hermes-base	default (sys-firewall)	200.7 MiB			
sys-firewall	default-dvm	sys-net	1.23 MiB			
sys-whonix	whonix-gateway-17	sys-firewall	220.98 MiB			
default-dvm	fedora-39-xfce	default (sys-firewall)	0.0 MiB			
hermes-dvm	hermes-base	default (sys-firewall)	0.0 MiB			
whonix-workstation-17-dvm	whonix-workstation-17	sys-whonix	0.0 MiB			
debian-12-xfce	Template/VM	default (n/a)	5607.83 MiB			
fedora-38-xfce	Template/VM	default (n/a)	5370.47 MiB			
fedora-39-xfce	Template/VM	default (n/a)	4877.11 MiB			
hermes-base	Template/VM	default (n/a)	4877.11 MiB			
whonix-gateway-17	Template/VM	default (n/a)	2206.31 MiB			
whonix-workstation-17	Template/VM	default (n/a)	3443.3 MiB			

HERMES backend components as qubes: HAPI, HDM, HDS, HDX, HUI