Product Bulletin 112

6-00960-189, Rev. A, October 2026

Bulletin Reference	ECE-2701
Title	Severity 5 Security Scan Findings and Stability Fixes in USP 5.3.1: Apply USP 5.3.1 Patch1
Affected Product	Unified Surveillance Platform (USP)
Affected Versions	USP 5.3.1 and earlier.
Fixed In	USP 5.3.1 Patch1 (applies to USP 5.3.1; the USP version continues to report QMCO_USP-5.3.1-241203).
Severity	**Security:** three findings rated **Severity 5** by vulnerability scanning tools (no evidence of active exploitation). **Stability:** addresses conditions that, in some scenarios, can lead to high memory usage or affect data-service availability.

Summary

Routine vulnerability scans of Unified Surveillance Platform (USP) systems report three findings rated **Severity 5**. Quantum has released **USP 5.3.1 Patch1**, which addresses these findings and delivers stability improvements for memory usage, iSCSI storage path recovery, and node-add and node-replace operations.

The patch is delivered as a standard upgrade package through the USP dashboard upgrade page. It does not upgrade any product component, and there is no downtime for virtual machines, storage, or virtualization services. Quantum recommends that all customers running USP 5.3.1 apply the patch at the earliest opportunity.

Issue 1: Severity 5 Security Scan Findings

Routine vulnerability scans of USP systems report the following findings, each rated **Severity 5**. None show evidence of active exploitation.

1. **OpenSSH ssh-agent Remote Code Execution (CVE-2023-38408 / QID 38904)**
   This finding is reported based on the OpenSSH version string. The patch disables SSH agent forwarding as an additional mitigation.
2. **Memcached Accessible Without Authentication (QID 38760)**
   The internal caching service is reachable from outside the cluster without credentials.
3. **VNC/SPICE Console Accessible Without Authentication (QID 38161)**
   Virtual machine console ports, used for local administrative access, are reachable on a routable interface.

Issue 2: Monitoring Data Exporter Memory Growth

Each USP node runs a monitoring data exporter that checks the virtual machines every 15 seconds and feeds the USP dashboards. Due to a defect in the exporter, a small amount of memory is not released after each check, so memory usage could grow continuously over time.

Impact: Memory growth of approximately 250–360 MB per node per day has been observed in some scenarios, increasing with the number of virtual machines. Left unattended over an extended period, this reduces the memory available to workloads and can affect node performance.

© Quantum Corporation. All rights reserved. Your right to copy this manual is limited by copyright law. Making copies or adaptations without prior written authorization of Quantum Corporation is prohibited by law and constitutes a punishable violation of the law. Quantum specifications are subject to change.

Issue 3: iSCSI Rescan Loop After SAN Network Link State Changes

When a SAN link on a node comes back up after a link down event, a background task instructs every node to rescan its iSCSI storage connections. Under certain conditions, these rescans can repeat across the cluster instead of completing once.

Impact: If concurrent rescan activities stack up and experience hangs, processes can accumulate on each node, causing memory pressure and storage path churn that can affect data-service availability.

Issue 4: Field Fixes Not Retained After Node-Add or Node-Replace

Impact: A node-add or node-replace operation can remove fixes previously applied to the running dashboard, including the fix for Issue 3. The operation reports success, so the original issue may recur without warning.

Resolution: USP 5.3.1 Patch1

USP 5.3.1 Patch1 makes the following changes:

- **Security hardening (Issue 1):** VNC/SPICE, memcached, and RabbitMQ ports answer only other nodes in the cluster, and SSH agent forwarding is disabled. Dashboard, virtualization, and virtual machine access are unaffected.
- **Monitoring memory (Issue 2):** the monitoring data exporter is limited to 1 GiB of memory and restarts automatically when it reaches the limit, so its memory use no longer grows.
- **iSCSI rescan (Issue 3):** each node performs a single local storage login after a SAN link state change, with no cluster-wide repetition.
- **Field fixes retained (Issue 4):** fixes present in the running dashboard are carried forward on all future node-add and node-replace operations. These workflows are also updated so the new security settings are applied correctly to added or replaced nodes.

Built-in safety checks: before changing any file, the patch verifies the exact file or line it is about to modify. If it finds a non-standard USP version or a hand-edited file, it stops and leaves that node untouched.

Impact of Applying the Patch

- No downtime for virtual machines, storage, or virtualization services. The dashboard remains available throughout.
- The patch reloads the SSH service, restarts the monitoring data exporter on each node (a gap of a few seconds in metrics), and adds firewall rules that affect no legitimate traffic.
- The patch takes about one minute to apply on a three-node cluster.

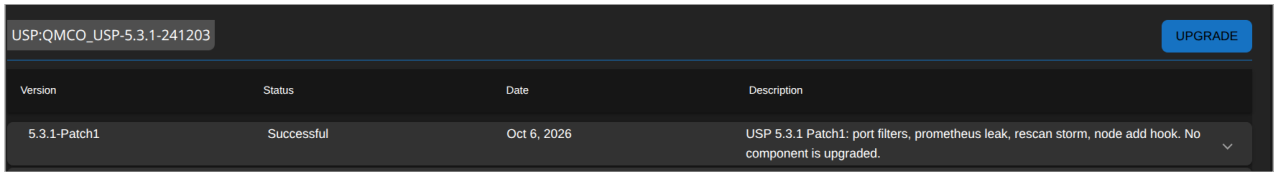
How to Apply

1. Obtain the **USP 5.3.1 Patch1** upgrade package from https://mysoftware.quantum.com/forms/usp.
2. Log in to the USP dashboard and open the upgrade page.
3. Upload and apply the **USP 5.3.1 Patch1** package as you would a standard upgrade package.
4. Wait for the patch to complete on all nodes (about one minute on a three-node cluster). If the patch reports that it could not be applied on a node, contact Quantum Technical Support.

© Quantum Corporation. All rights reserved. Your right to copy this manual is limited by copyright law. Making copies or adaptations without prior written authorization of Quantum Corporation is prohibited by law and constitutes a punishable violation of the law. Quantum specifications are subject to change.

Confirming the Patch Is Applied

1. **Check the dashboard upgrade page:** The upgrade page lists **5.3.1-Patch1** with a status of **Successful**, the date it was applied, and a description of the patch, as shown in the example below.



Example: USP dashboard upgrade page after USP 5.3.1 Patch1 is applied.

Note: The USP version shown at the top of the page remains **QMCO_USP-5.3.1-241203** after the patch is applied. This is intentional and prevents a version mismatch during future node-add and node-replace operations.

2. **Rescan with your vulnerability scanning tool** to confirm that the Severity 5 findings (QID 38904, QID 38760, and QID 38161) are addressed.
3. **Optional detailed check (or with Quantum Technical Support):** the upgrade leaves a copy of the package at `/var/lib/upgrades/USP_5.3.1_Patch1` on one of the cluster nodes. Log in to that node and run:

```
cd /var/lib/upgrades/USP_5.3.1_Patch1
python3 testing/verify_patch.py
```

The script checks every node and ends with a verdict line, for example `verify: 3/3 nodes PASS`. If any node reports FAIL or is unreachable, contact Quantum Technical Support.

Important Operational Notes

- **Re-apply after every node-add or node-replace.** The patch package must be re-applied after any node is added or replaced. The re-application changes only the new node.
- **Expected monitoring restarts.** Once the patch is applied, the monitoring data exporter restarts itself every few days when it reaches its memory limit. This is expected and has no effect beyond a brief gap in metrics.
- **No rollback procedure.** This patch does not include a rollback procedure.

Recommended Action

- **Apply USP 5.3.1 Patch1** to all USP 5.3.1 systems at the earliest opportunity.
- **Systems running releases earlier than USP 5.3.1:** contact Quantum Technical Support for guidance.

References

Security findings: CVE-2023-38408 / QID 38904, QID 38760, QID 38161.

Tracking: ECE-2701 (this bulletin).

If needed, contact Quantum Technical Support to obtain additional assistance with applying this patch.

© Quantum Corporation. All rights reserved. Your right to copy this manual is limited by copyright law. Making copies or adaptations without prior written authorization of Quantum Corporation is prohibited by law and constitutes a punishable violation of the law. Quantum specifications are subject to change.