

Two Critical MarkLogic Flaws Enable Privilege Escalation to Administrator Control



Progress Software disclosed 31 vulnerabilities in MarkLogic Server, including two critical flaws that allow delegated managers to gain persistent administrator control. Patches were released in September.

- Progress Software disclosed 31 vulnerabilities in MarkLogic Server on October 12, with five rated critical severity
- Two critical flaws enable accounts with limited management privileges to escalate to full administrator control
- Security patches have been available since September 10 in versions 11.3.7 and 12.1.0
- The vulnerabilities affect database systems that may handle sensitive regulated data

Progress Software has disclosed 31 security vulnerabilities in its MarkLogic Server database platform, including two critical flaws that permit **privilege escalation** from delegated management accounts to full administrator control. The vendor published the advisory on October 12, rating five of the vulnerabilities as critical severity.

Vulnerability Details

The two most serious flaws allow user accounts that have been granted limited management privileges to escalate their access and obtain persistent administrator-level control over the MarkLogic Server instance. This type of privilege escalation represents a significant risk for organizations that rely on role-based access controls to protect sensitive data stored in database systems.

Patches Available Since September

Progress Software released security updates addressing all 31 vulnerabilities on September 10, ahead of the public disclosure. The fixes are included in MarkLogic version 11.3.7 and version 12.1.0. Organizations running earlier versions remain exposed to potential exploitation.

Implications for Regulated Institutions

For financial institutions, healthcare providers, and other regulated entities in the Kingdom that deploy MarkLogic Server for data management, these vulnerabilities pose compliance and operational risks. Database systems often store customer records, financial transactions, and other sensitive information subject to regulatory protection requirements. Unauthorized administrator access could lead to data breaches, unauthorized modifications, or compliance violations under applicable frameworks.

What to do now

1. Identify all MarkLogic Server instances in your environment and verify current version numbers against the vendor advisory
2. Prioritize immediate patching to version 11.3.7 or 12.1.0 for all production and non-production MarkLogic deployments
3. Review audit logs for any unusual privilege escalation activity or unauthorized administrative actions since September
4. Validate role-based access control configurations and restrict delegated management privileges to the minimum necessary
5. Document patching activities and version updates for compliance evidence under NCA ECC and SAMA frameworks
6. Coordinate with application owners to schedule maintenance windows if patching requires service interruption