Docker Buster Security Report

Image Information

Image: nginx:1.19

Scan ID: 6ccfd394-1843-4e84-b965-43561d9351cf

Scan Date: 2025-05-12 21:21:33

Executive Summary

10.0

CRITICAL RISK

505
CVEs Found

0
License Issues

No
Secrets Detected

603
Components

Vulnerability Severity Breakdown

Severity	Count	Description
Critical	51	Vulnerabilities that require immediate attention

High	181	Vulnerabilities that should be prioritized
Medium	231	Vulnerabilities that should be addressed
Low	42	Low impact vulnerabilities

License Compliance: No license issues detected

Component Details

SBOM Summary

This image contains 603 components.

Top Vulnerable Components

Name	Version	Critical	High	Total
apt	1.8.2.3	0	0	1
bash	5.0-4	0	0	1
bsdutils	1:2.33.1-0.1	0	0	3
bsdutils	1:2.33.1-0.1	0	0	3
bsdutils	1:2.33.1-0.1	0	0	3

Actionable Insights

Recommended Actions

1. Update vulnerable packages to their latest versions
2. Review and resolve license compliance issues
3. Implement proper secrets management practices
4. Consider using minimal base images
5. Regularly scan your containers for new vulnerabilities

Upgrade Recommendations

Component	Current Version	Recommended Version	Priority

Security Best Practices

- Use multi-stage builds to reduce image size and attack surface
- Avoid running containers as root
- Never hardcode secrets in Dockerfiles or environment variables
- Keep your base images updated
- Implement image signing for supply chain security

Verification Information

SHA-256:
01e377bdf2490b4cdcce73e3105bb83868343d99e757d1d69657f40f8d4ab029