



December 7, 2020

MechCentral Security Assessment

IOActive was engaged to perform a white-box security assessment of the MeshCentral open-source remote management software. Both MeshCentral¹ and MeshAgent² were in scope for this assessment, which covered:

- Evaluating the software against industry best practices
- Covering well-known attacks against standards-based features
- Identifying new attack vectors specific to this product

Four IOActive consultants audited the source code available on GitHub from the 15th of June to the 17th of July 2020, for a total of 480 resource hours.

The following tasks were performed as part of the source code review:

- Attack Surface Analysis
- Dependency Analysis
- Common Coding Errors
- Dataflow Analysis
- Security-critical Code
- Static Analysis
- Language-neutral Issues
- Language-specific Issues

¹ <https://github.com/Ylianst/MeshCentral>

² <https://github.com/Ylianst/MeshAgent>



Results: IOActive identified 22 critical-risk, 24 high-risk, 36 medium-risk, 21 low-risk, and nine informational vulnerabilities across both projects.

Subsequently, IOActive was engaged to perform remediation validation testing. One IOActive consultant retested the reported findings from the 19th of October to the 6th of November 2020.

MeshCentral's Response to the Findings: MeshCentral will issue a separate statement in response to the findings.

Respectfully,

DocuSigned by:

Jennifer Steffens

E0FA5D8E7A2D46C...

Jennifer Steffens

Chief Executive Officer

IOActive, Inc.

DS

IOA LCA Approved - KM



IOActive Qualifications

IOActive has more than 20 years of experience providing information security consulting services. Established in 1998, IOActive is an industry leader that specializes in:

- IT infrastructure vulnerability assessments and pen tests
- Application security source code and architecture reviews
- ICS/SCADA and smart grid assessments and pen tests
- Emerging market assessments and pen tests (cloud, embedded, automotive, and more)
- Security development lifecycle training and review

IOActive works with many Global 500 companies including organizations in the power and utility, industrial, game, hardware, embedded, retail, financial, media, travel, aerospace, healthcare, high-tech, social networking, cloud, and software development industries.

We provide unequalled technical services, strive to become trusted advisors to our clients, and help them achieve their business and security objectives. We go well beyond off-the-shelf code scanning tools to perform gap analysis on information security policies and protocols. We also conduct deep analyses of information systems, software architecture, and source code using leading information risk and security management frameworks and focused threat models.

Your opponents do not use unsophisticated commercial pen-test tools to undermine your enterprise security. They use the smartest code breakers money can buy to footprint and damage your organization's brand using advanced, often unknown methods. IOActive's industry experience helps our clients consistently stay ahead of tomorrow's threats.

IOActive attracts people who contribute to the growing body of security knowledge by speaking at elite conferences such as RSA, SANS, SOURCE, Black Hat, InfoSecurity Europe, DEF CON, Blue Hat, and CanSecWest. We also have key advisors like Steve Wozniak and David Lacey, luminaries who affect how security and technology shape our world.