Security Assessments and Audits Assurance Letter

Penetration Tests

Micro Focus performs several types of security tests, some as part of its product lifecycle, and some against the supporting infrastructure.

All Micro Focus SaaS products considered as high criticality products and as such required to go through two types of PT:

Application PT

As part of the product SDLC process, every version release is tested by a third party company against the following type of attacks:

- Unauthorized access to sensitive information
- Unauthorized modifications of information
- Unauthorized deletion of information
- Performance of unauthorized operations or transactions
- Illegal or unauthorized impersonation to different users or entities
- Performance of unauthorized operations that may affect system's SLA
- Performance of unauthorized operations that may cause Denial-of-Service
- Exploitation of existing security controls to perform fraudulent activities

The following scenarios are simulated on critical product Web Interfaces and significant product features trying to exploit vulnerabilities in the design, implementation or deployment of mechanisms such as:

- End user Authentication mechanisms
- User and Password management mechanisms
- Access Control, RBAC and Permission related mechanisms
- Input Validation mechanisms
- Output Encoding mechanisms
- Session Management mechanisms
- Data protection mechanisms in transport and at rest
- Auditing and tracking mechanisms
- Security hardening of 3rd Party / FOSS components and libraries

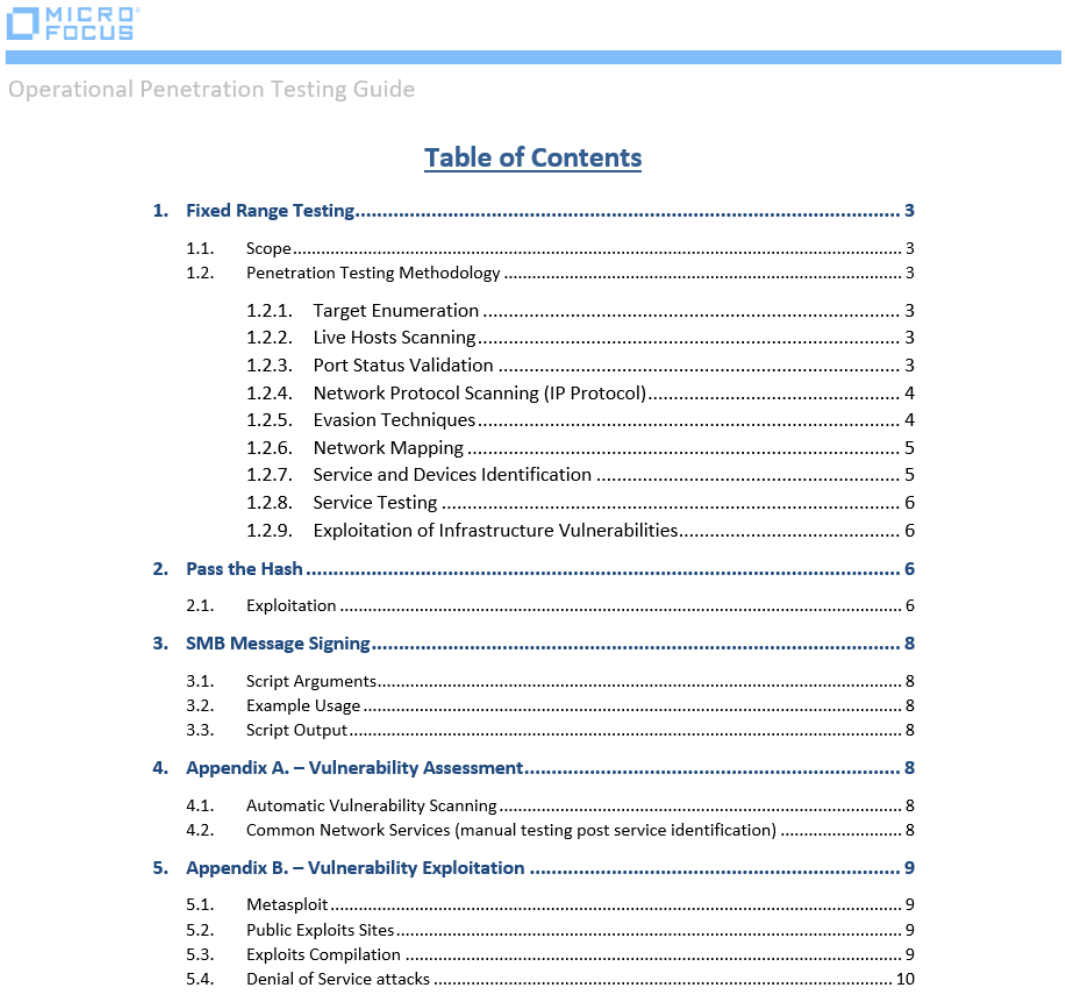
The following privacy scenarios are tested to cover compliance with data protection and privacy legislative requirements:

- Person-based and sensitive information is stored correctly
- Person-based and sensitive information can be exported by the application to comply with data portability legal requirements
- User activity is logged and date stamped for monitoring purposes
- Access control to sensitive information is clearly recorded
- Data retention mechanisms are embedded where applicable

The assessment findings are being remediate according to our SDLC program SLA's, critical findings where mitigated immediately, and a patch is released.

Operational PT

Every SaaS product required by policy to conduct an annual operational PT against its infrastructure, the test is conduct by a third party company and following Micro Focus OPT guide (ToC screenshot below).



Operational Penetration Testing Guide

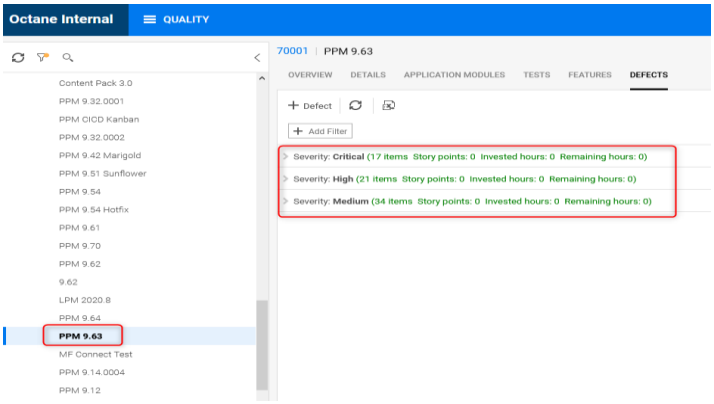
Table of Contents

Security defects management system

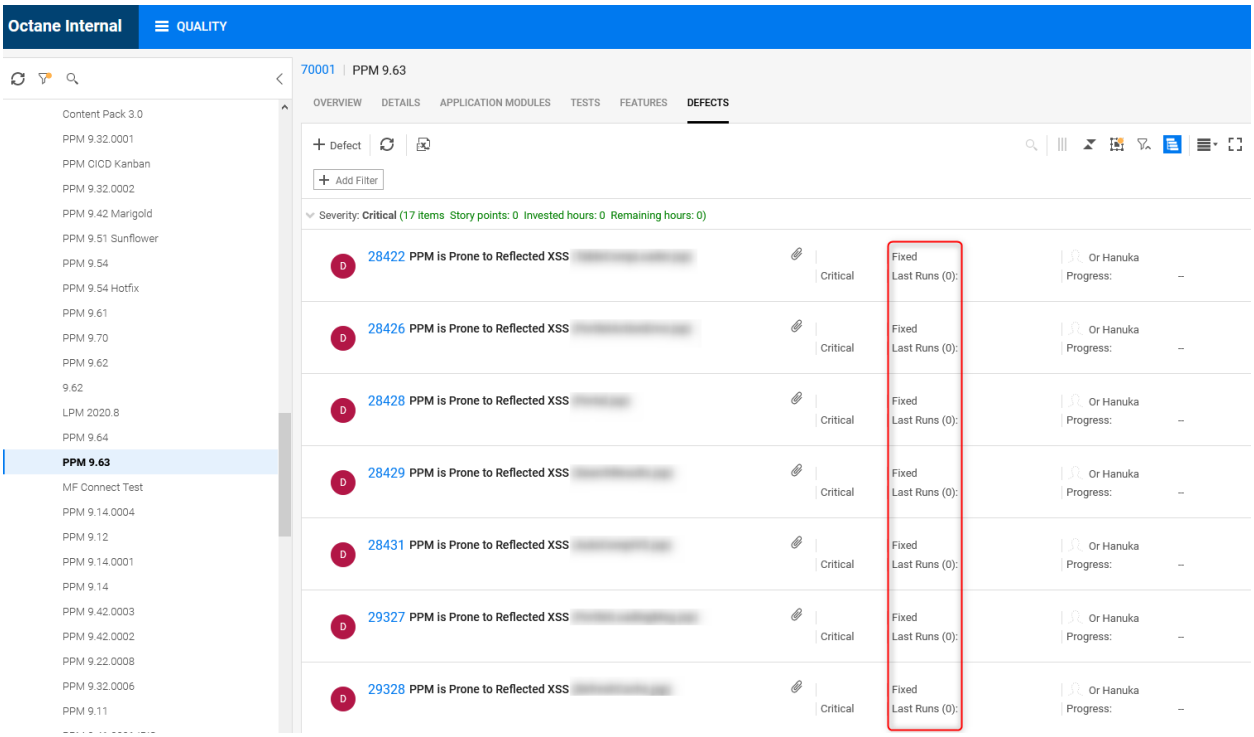
Micro Focus utilized Octane as its Security defects management system, the system is being updated by the external testers and the product security leads follow up on remediation with the R&D team.

Once all the "critical" and "high" findings has been remediated, the process move the sign off stage that at the end of it the version will be approved and released.

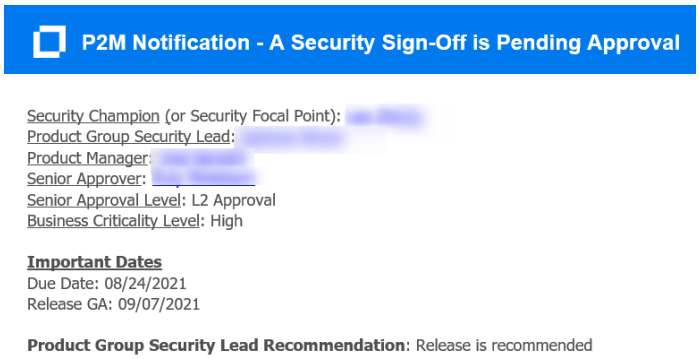
The following image showing the version security defects summary:



The following image showing the findings status:



The following image shows the signoff pending approval notification (sent to the Product Ops Security Officer):

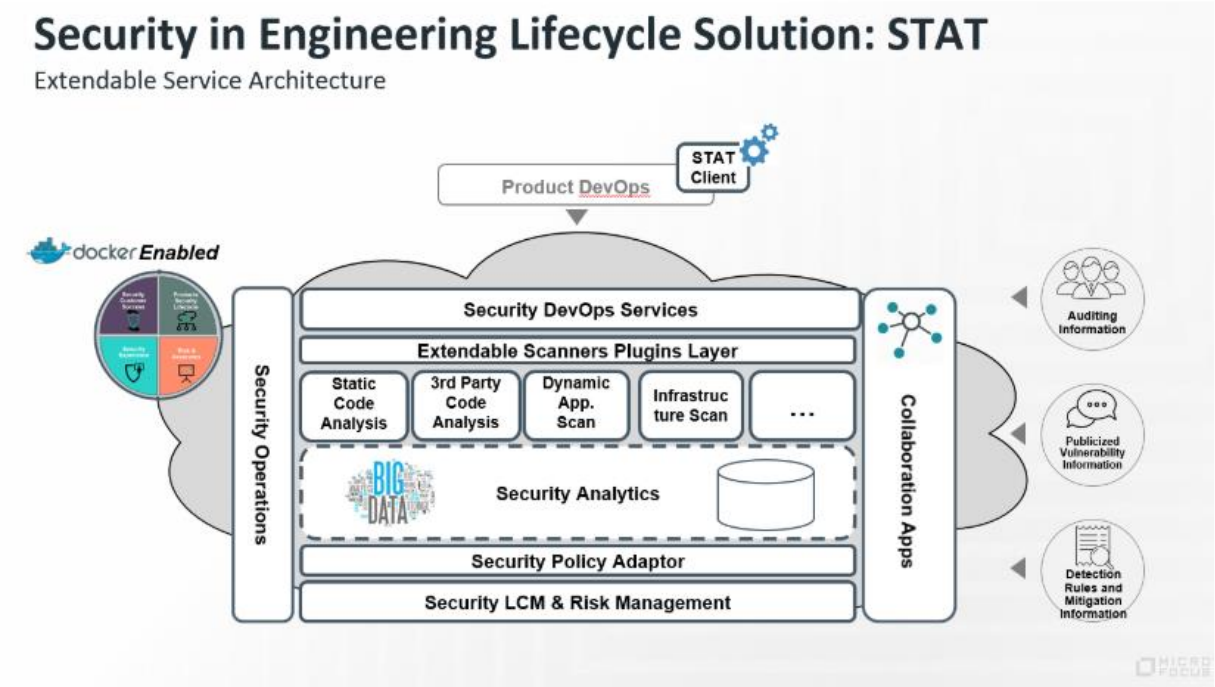


Automatic Security Testing platform for Agile and DEVOPS

Micro Focus conduct automatic scans with internal platform called STAT.

STAT is an Automatic Security Testing platform for Agile and DEVOPS, used daily to automatically scan source code and apps, and intercept new vulnerabilities in a near-real-time manner.

The following tools are part of these scans: Webinspect, OWASP Dependency, Checker, CoreOS Clair, Fortify and Nessus.



Vulnerability Scans

A monthly vulnerability scan is performed to assess OS and network components for known weaknesses & vulnerabilities. This is being done by “Qualys”, a remote security scanning tool, which scans the target and raises an alert if it discovers any vulnerabilities associated with this target.

Patching is done according to our Patch Management Program.

Emergency updates will be performed as soon as possible after ensuring patch stability and within six days. These updates should only be applied if they fix an existing problem that the server is experiencing.

Critical updates should be applied during off hours within seven days’ time frame after ensuring patch stability and an emergency CAB.

Non-critical updates on non-critical systems will be performed on regular scheduled maintenance windows within a two months period.

Internal and External Audits

As the seventh largest pure-play software company in the world we have more than 20 audits per year, Micro Focus management committed for delivering information & application security across its product portfolio.

ITOM/ADM products Internal Audits

As part of our compliant management program, ITOM/ADM has been audited in July 2021 by OranSec against the following controls:

- Leadership and commitment
- Organizational roles, responsibilities and authorities
- Information security risk assessment
- Information security risk treatment
- Information security objectives and planning to achieve them
- Competence
- Awareness
- Creating and updating of documented information
- Control of documented information
- Operational planning and control
- Information security risk assessment.
- Information security risk treatment
- Monitoring, measurement, analysis and evaluation
- Management review
- Nonconformity and corrective action
- Continual improvement.
- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control

Grant Thornton performed another short assessment for ITOM/ADM SaaS products in August 2021 against the SOC 2 type II controls.

ITOM/ADM products External Audits

Micro Focus ITOM and ADM have been certified for ISO27001 and ISO27034 for nineth years in a row.

The last certification cycle completed in 2020 conducted by Schellman.

The SOC2 type II certification renewal started in June 2021 lead by Grant Thornton.

Our continuous certification clearly demonstrates Micro Focus' commitment to deliver secure products to our customers.

Sincerely,

Snir Karat
Product Operations Security Officer