



CERTIFICATE

OUTLOOKMOVIE s.r.o.

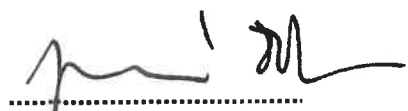
Scope of the test:

External testing of OutlookMovie infrastructure and environment vulnerabilities accessible from the Internet in the test environment.

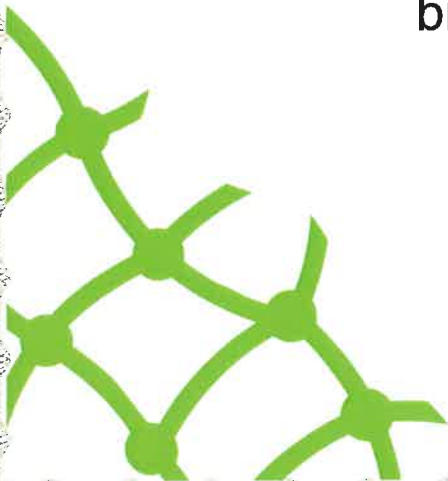
Test result:

The developer.outlookmovie.com information system does not contain critical security weaknesses that could lead to a data breach of authorized users.

12 June 2024



Ing. Jaromír Žák
Director NGSS



The test was based on the following criteria:

- Open Source Security Testing Methodology Manual,
- The Open Web Application Security Project,
- NIST 800-115,
- Common Vulnerability Scoring System,
- Center for Internet Security Benchmarks.

SCOPE OF WORK:

"Security test"

PRO:

OUTLOOKMOVIE S.R.O.

9 MAY 2024

Next Generation Security Solutions s.r.o.
U Uranie 954/18, Prague 7, 170 00

Tel: 237 836 950

sales@ngss.cz | www.ngss.cz

1. Identification of the test supplier

Next Generation Security Solutions s.r.o.	
Headquarters:	U Uranie 954/18, Holešovice, 170 00 Prague 7
ID:	06291031
TIN:	CZ06291031
File mark	C 279627 registered at the Municipal Court in Prague
Legal form:	Limited Liability Company
Statutory body:	Mgr. Ondřej Dedek, Managing Director
Website:	www.ngss.cz
Contact person:	Daniel Přivratský service manager +420 603 298 132 dprivratsky@ngss.cz

2. Table of Contents

1.	Identification of the test supplier	1
2.	Table of Contents	2
3.	Preamble to the security test	4
4.	Basic information about the test	5
4.1.	<i>Test timeframe</i>	5
4.2.	<i>Purpose and scope of the tests</i>	5
4.3.	<i>Connection method</i>	5
4.4.	<i>Information about the implementation team</i>	6
4.5.	<i>Contact persons for the tested organization</i>	6
4.6.	<i>Excluded controls from the security test</i>	6
4.7.	<i>Other limitations of the security test</i>	6
5.	Test methodology	7
5.1.	<i>Vulnerability test</i>	7
5.1.1.	Preparation	7
5.1.2.	Collection of information	8
5.1.3.	Vulnerability enumeration and analysis	8
5.1.4.	Reporting	8
5.1.5.	Measures to minimize risks	8
5.2.	<i>Testing and evaluation standards</i>	9
5.2.1.	OSSTMM	9
5.2.2.	OWASP	10
5.2.3.	NIST Special Publication 800-115 and 800-44	10
5.2.4.	CVSS	10
5.3.	<i>Tools used</i>	10
5.3.1.	Awareness of testers	11
5.3.1.1.	Black box	11
5.3.1.2.	Gray box	11
5.3.1.3.	White box	11
5.4.	<i>Risk minimization measures</i>	11
5.5.	<i>Final report</i>	12
6.	Test parameters	13
6.1.	<i>Setting the environment</i>	13
6.2.	<i>Setting the environment</i>	13

6.3.	<i>Technical parameters and course of the penetration test</i>	13
6.4.	<i>Monitored values</i>	13
6.4.1.	Testing party	13
6.4.2.	Tested party	13
6.4.3.	Monitoring of the test progress	13
6.5.	<i>Time course of the test</i>	14
6.5.1.	Internal vulnerability test	14
6.5.1.	Test report	14
6.6.	<i>Access data</i>	14
6.7.	<i>Communication scenario and test environment supervision</i>	14
6.7.1.	Risk of infection by malicious code	14
6.7.2.	Risk of leakage of sensitive data	14
6.7.3.	Contact persons	15

3. Preamble to the security test

This document, which forms the terms of reference for the security test, defines the test methodology and procedures, including the oversight of the test, the management of contingencies, exceptions and limitations that will be taken into account during testing. It is also used for mutual agreement and confirmation of the vulnerability test.

The test will be conducted using automated tools for scanning vulnerabilities in ICT and OT technologies and services, followed by manual verification, with the aim of mapping the maximum possible number of potential vulnerabilities and security weaknesses resulting from missing security patches for known vulnerabilities and/or insufficient configuration of operating systems and application software.

Due to the sensitivity of the testing, it is necessary to fix the test rules in this document in such a way that the test is performed in a predefined form and quality, thus minimizing potential risks.

4. Basic information about the test

4.1. Test timeframe

The timing of the OutlookMovie security test (hereinafter referred to as the "Client") will be specified prior to the start of the test.

4.2. Purpose and scope of the tests

The security test will consist of:

- External vulnerability test;

The tested environment will include:

- OutlookMovie infrastructure and environment accessible from the Internet in the test environment

The aim of the security test will be to check whether:

- unauthorized access to services/data/systems can be gained,
- unauthorized modification/destruction of data passing through the communication infrastructure or processed/stored on systems,
- can be penetrated by security features,
- you can obtain authentication data or escalate permissions within the application
- the infrastructure can be exploited to attack third-party networks and services; and
- there are vulnerabilities that can lead to the previous points.

Vulnerability testing will always be performed in these areas using the current available databases of vulnerabilities and flaws in the implementation or configuration of individual technologies:

- defined IP range,
- network infrastructure,
- security feature,
- HW server/workstation,
- virtualization platforms,
- Microsoft Windows / Linux OS.

The aim of the review will be to identify potential security weaknesses and propose effective measures to eliminate them, including prioritizing their implementation. A combination of multiple testing methods will be used to assess, to the maximum extent possible, the level of security of all components of the tested scope of the information system from all available vectors.

The test will be performed without access to the application source code. A set of basic access permissions will be available to the tester.

4.3. Connection method

The security test will be performed using a standard Internet connection available to public Internet users in the Czech Republic and abroad.

4.4. Information about the implementation team

The implementation team will be composed of the following persons listed in the table and will not be changed during the tests.

Name and surname	Role in the team	Contact phone
Daniel Přivratský	Service Manager	+420 603 298 132
Jan Novák	Tester	+420 722 466 963

4.5. Contact persons for the tested organization

The contacts for the tested organization will be specified before the start of the test.

4.6. Excluded controls from the security test

The tests performed will exclude any tests that could result in permanent limitation or other impairment of the availability of the services of the tested systems.

4.7. Other limitations of the security test

No other restrictions are imposed.

5. Test methodology

The chapter describes in general terms the implementation of the different phases of the security test in the "black-box" and "gray-box" mode, which means that we perform the test from the Internet environment exactly as cyber criminals would do it, possibly with a limited amount of information and cooperation of the tested organization. Thus, a realistic attack scenario tests not only technical preparedness but also the human factor in the context of the tested organization's cybersecurity.

5.1. Vulnerability test

Vulnerability scanning is mainly carried out using automated tools for vulnerability scanning in ICT and ICS technologies and services with the aim of mapping the maximum possible number of potential vulnerabilities and security weaknesses resulting from missing security patches for known vulnerabilities and/or insufficient configuration of operating systems and application software.

For the majority of modern technologies, vulnerability scanning does not pose a higher risk of negative impact on their operation, however, depending on the types of devices and application software that are in the defined range for the vulnerability scanning, it may be recommended to exclude certain types of devices and application software from automated vulnerability scanning, in particular printers, disk arrays, UPS, IP camera, etc.

These are usually non-standard IT technologies and ICS elements that are not designed to actively scan for vulnerabilities using automated tools, where their use can lead to unavailability or non-standard device behavior.

Vulnerability scanning will always be performed in these areas using the current available vulnerability databases and vulnerabilities in the configuration of each technology:

- defined IP range,
- network infrastructure,
- security feature,
- HW server/workstation,
- virtualization platforms,
- Microsoft Windows OS,
- Linux OS.

5.1.1. Preparation

The preparatory phase establishes the scope, method and type of vulnerability scanning, including other rules for the implementation of vulnerability scanning, in particular:

- Explicit specification of the scope of vulnerability scanning,
- type of vulnerability scan, i.e. black box, gray box or white box,
- The method of performing the vulnerability scan, i.e., authenticated or unauthenticated,
- the appointment of a coordinator on the organization's side,
- security requirements for suppliers (limitations on testing from a security and operational perspective),
- the details and format of the report,
- dates and schedule for the implementation of vulnerability scanning,
- depending on the type of scan and the availability of information, are defined at this stage or for the information gathering phase:
 - vulnerability scanning scenarios,
 - a list of techniques and tools used to perform the scan,

- the scanning method for each technology,
- the possible negative impact of scanning on technology and the resulting limits on the vulnerability enumeration techniques used,
- requirements and rules for interaction,
- escalation procedures,
- protection and handling of personal data,
- rules for defining and communicating significant findings during the vulnerability scanning process.

5.1.2. Collection of information

In this phase, the behavior of the attacker and his techniques is simulated in the initial phase of gathering information about the target of the cyber-attack using OSINT (Open source intelligence) and analyzing this information to select appropriate techniques during the vulnerability enumeration phase. This phase can be omitted entirely or implemented to a limited extent if the vulnerability scanning is of the white box or gray box type.

5.1.3. Vulnerability enumeration and analysis

Based on the information provided or discovered, this phase involves the selection of appropriate techniques for the enumeration of known vulnerabilities in the tested technologies or their configurations. The techniques are chosen in such a way as to minimize the negative impact on the technologies under test.

If at this stage it is not possible to enumerate, without excluding negative impact, vulnerabilities using active techniques with automated vulnerability scanners, a manual vulnerability enumeration procedure is recommended. A similar approach is followed if the necessary enumeration cannot be achieved using automated tools due to their limitations.

If potentially critical vulnerabilities are found, the vulnerabilities found can be manually verified at this stage in agreement with the responsible personnel of the organization.

5.1.4. Reporting

At this stage, a final report is prepared listing the vulnerabilities found, including a severity level classification, and recommended countermeasures to eliminate or minimize the risks, including their prioritization.

Where possible, we always recommend a possible way of immediately remediating vulnerabilities in the short term, as well as strategic measures leading to the elimination of the same or similar type of vulnerability in the long term.

The vulnerability scan, its progress, findings and proposed measures are also presented to the organization's employees.

Further information on the structure and content of the document can be found in the Final Report chapter.

5.1.5. Measures to minimize risks

Although the automated scanning of most current technologies has no or minimal negative impact on the occurrence of vulnerabilities, for some technologies a negative impact cannot be completely eliminated; in order to minimize the negative impact, we choose the following practices in particular:

- Early notification of technologies to be scanned for vulnerabilities that are known to be at increased risk of negative impact and recommendation of an alternative vulnerability enumeration process.

- Setting up automated vulnerability scanning tools in such a way that testing minimizes the resources required on the side of the technologies under test.
- Vulnerability scanning is done in parts.
- In the case where it is possible to perform vulnerability scanning as a white box test without negatively affecting the result of the test, we always recommend performing vulnerability scanning in this way.
- In the case where it is possible to perform vulnerability scanning in a test environment without negatively affecting the result of the test, we always recommend performing it in a test environment.
- If it is discovered during the penetration testing that the infrastructure and applications under test have been targeted and compromised in the past, the penetration testing will be suspended until the incident is resolved. The organization's company representative will be informed immediately.

5.2. Testing and evaluation standards

The security testing methodologies used by consultants are based primarily, but not exclusively, on the following methodologies, which are categorized as "best practice" for different types of security testing across different sectors:

- Open Source Security Testing Methodology Manual,
- The Open Web Application Security Project,
- NIST 800-115 and 800-44,
- Common Vulnerability Scoring System,
- Center for Internet Security Benchmarks,
- security recommendations from individual technology suppliers,
- and others.

5.2.1. OSSTMM

The supplier uses the internationally recognized standard OSSTMM - Open Source Security Testing Methodology Manual as the basis for security testing (including penetration tests).

This methodology was developed at the Institute for Security and Open Methodologies - www.isecom.org and is continuously developed by a large group of professional testers and ICT security specialists.

The OSSTMM methodology covers the execution of penetration tests in any environment where the tester has the same rights as a normal user. By verifying all areas that are defined in OSSTMM, a complete penetration test is performed on the system.

The OSSTMM does not prescribe the form or depth of the tests to be performed. The methodology focuses on defining the basic models of testing, the main areas of testing and how to present the results.

The methodology is based on the OSSTMM and is continuously updated to reflect best practices in ICT security and security testing today. The most important sources of the methodology are:

- ISO/IEC 27000 series standards,
- OWASP (Open Web Application Testing Standard - www.owasp.org),
- NIST (National Institute of Standards and Technology - www.nist.gov - only documents related to testing, setting up and operating ICT security).

The OSSTMM methodology defines the recommended range of tests to be performed. The contractor's security testing staff continuously develops, maintains and catalogues an extensive

database of knowledge and specific procedures. These practices and knowledge cover all the most commonly used operating systems, applications, network protocols and general ICT theory.

5.2.2. OWASP

The testing of web applications is based on methodologies that come from the OWASP project (www.owasp.org - The Open Web Application Security Project). OWASP includes many different services, such as the "OWASP Testing Guide", the "Guide to Building Secure Web Applications and Web Services", the OWASP TOP TEN project, testing tools, the "OWASP Web Application penetration checklist" and many more.

The OWASP Testing Guide version 4 is used to test and present the results of web application security tests.

Secure Code Review is implemented according to the OWASP Code Review Guide v2.

5.2.3. NIST Special Publication 800-115 and 800-44

NIST SP 800-115 and 800-44 recommendations are used as an auxiliary methodology for organizing testing in some selected parts, namely:

- Information security assessment, including policies, roles and responsibilities, methodologies and techniques used,
- Identifying targets and analyzing them for potential vulnerabilities, including network search techniques and vulnerability scanning,
- verifying the existence of vulnerabilities,
- coordination, evaluation, analysis and data processing.

5.2.4. CVSS

The identified vulnerabilities are ranked according to importance. For this purpose, the CVSS (Common Vulnerability Scoring System) metric is used, which is an industry standard for rating the severity of vulnerabilities in information systems. The development of this CVSS metric is overseen by the Forum of Incident Response and Security Teams (FIRST). The current methodology used in the assessment is version 3.1.

The CVSS metric makes it easy to distinguish critical vulnerabilities from less important ones by scoring vulnerabilities on a scale of 0 to 10, with 0 being low and 10 being high. The assessment itself is then carried out in several steps and is based on a series of measurements oriented towards different groups of characteristics of a given vulnerability.

Vulnerabilities identified during a vulnerability scan or penetration test are classified according to the CVSS BMG (CVSSv3 Base Metric Group - <https://www.first.org/cvss/v3-1/>). This rating metric is chosen due to its worldwide acceptance in the security community and provides a balanced view of the overall vulnerability classification.

CVSS BMG captures the characteristics of the vulnerabilities found in eight basic metrics that are constant over time and independent of the environment where the application is running.

The use of CVSS metrics enables monitoring of trends in system vulnerabilities, matching with risks identified in risk analyses and other information within security management decision support systems.

5.3. Tools used

All the tools used meet several basic criteria that generally ensure greater security and confidence in the tests performed and reduce the risks involved in testing production systems.

All tools are thoroughly tested on their own polygon to verify their correct functioning, the actual functions performed and the possible impact on the tested and surrounding parts of the system.

All key tools are analyzed and compiled by the supplier's staff. Tools for which this is not possible are subject to increased testing and are used only for detection purposes and not in the phases of creating or maintaining access to the system under test.

In the case of the need to use special code to exploit an existing weakness (so-called exploit), custom programs or those that can be checked for source code and tested on a polygon are always preferred.

Most of these tools have no or minimal harmful impact on the actual systems tested. For tools where there is a higher risk but where the quality and added value of the tool cannot be replaced by any safer means, this is indicated. The use of these tools is always planned for times when production systems are not heavily used.

The main tools used in the client environment include:

- Nessus Professional,
- Hydra,
- Terrascan,
- Metasploit.

5.3.1. Awareness of testers

Before starting the tests, a procedure can be chosen, varying in the level of tester awareness, to simulate the role of the potential attacker as appropriately as possible.

5.3.1.1. Black box

Before performing a vulnerability scan or penetration test, our consultants have minimal information about the targets to be tested, e.g. only IP address, URL, etc. This type of test is particularly suitable for cases of simulating the behavior of an external attacker.

5.3.1.2. Gray box

Prior to conducting a vulnerability scan or penetration test, our consultants have a limited set of information about the targets to be tested, such as architecture, technologies and users, as well as basic access to the targets to be tested, e.g. at the legitimate user level. This type is particularly suitable for the case of simulating the behavior of an internal attacker with a limited set of information and user permissions.

5.3.1.3. White box

Before performing a vulnerability scan or penetration test, our consultants have all available information about the targets to be tested, e.g. full documentation, application source code, etc. They also have access to the tested systems at the privileged user level. This type is particularly suitable for testing where the maximum number of vulnerabilities need to be identified, including those that cannot be identified during black box or gray box testing.

5.4. Risk minimization measures

Although scanning most current technologies for vulnerabilities has no or minimal negative impact, for some technologies a negative impact cannot be completely ruled out. In order to minimize the negative impact, we choose the following practices in particular:

- Early notification of technologies to be scanned for vulnerabilities that are known to be at increased risk of negative impact and recommendation of an alternative vulnerability enumeration process,
- Setting up automated vulnerability scanning tools in such a way that testing minimizes the resources required on the side of the technologies under test,
- Vulnerability scanning is done in parts,
- in the case when it is possible to implement vulnerability scanning as a white box test without negatively affecting the result of the implemented test, we always recommend implementing vulnerability scanning in this way,
- in the case when it is possible to perform vulnerability scanning in the test environment without negatively affecting the result of the test, we always recommend performing it in the test environment,
- if it is discovered during the execution of the tests that the tested infrastructure and applications have been the target of an attack in the past and have been compromised by this attack, the execution of the tests will be suspended until the incident is resolved. The organization's company representative will be informed immediately.

5.5. Final report

A final report will be prepared from the security test in the following expected structure (the final structure may be modified by the tester to better reflect the test results).

- a management summary including a summary of findings and recommendations for action with an indication of prioritization of actions,
- basic information about the test, including timeframe, objectives, scope, technical data, test team details, test limitations, etc.,
- a test methodology describing the test phases and the metrics used so that the test can be repeated periodically, or the results verified,
- test results with statistical evaluation and detailed description of the findings in the tested range of systems, networks, etc.

6. Test parameters

6.1. Setting the environment

The external part of the test will be conducted remotely from the supplier's systems via the public internet network.

The tester's systems will perform time synchronization against a trusted time source before starting the tests.

The primary addresses reserved for tester devices are 31.30.70.42 and 145.224.105.184, or other addresses depending on the circumstances of the test.

6.2. Setting the environment

The test will primarily be conducted remotely from the Internet.

The IP address range to be tested will be provided by the client prior to the start of the test.

6.3. Technical parameters and course of the penetration test

The technical parameters with regard to the environment are set as follows:

- maximum number of simultaneously open connections - 10,
- maximum number of simultaneously tested systems - 5,
- maximum number of simultaneous tests per system - 2.

6.4. Monitored values

6.4.1. Testing party

On the tester's side, all results of the tests performed will be time-indexed and stored. The monitored results are the outputs of the nmap and nessus test tools. A complete record of the network communication between the auditor's system and the system under test will be made with the tcpdump tool and stored in a standard format for subsequent processing by the Ethereal analysis tool.

6.4.2. Tested party

The tested party is not bound by the obligation to monitor the progress of the test. However, the information stored in the standard System and Application logs by time index may have added value for retrospective analysis and event reconstruction after the campaign is over.

6.4.3. Monitoring of the test progress

During the test, the auditor will continuously monitor system availability at the ip stack level using icmp queries. In addition to the existence of responses, their latency will also be evaluated. At the same time, the tester will perform health checks of the applications under test to the best of his ability.

All of these values will be reported in the Final Test Report document if any response problems are found with the systems tested.

6.5. Time course of the test

The following timetable has been developed based on empirical best-practice methods and according to the capabilities of the organization.

Time T is the time of acceptance of the binding order. The dates assume the client's cooperation in making the premises available and providing Ethernet connectivity.

6.5.1. Internal vulnerability test

Testing will begin in T+14 days.

Estimated completion is within T+21 days.

6.5.1. Test report

The final summary report of the tests performed will be provided to the client within T+31 days.

In the event of a successful penetration or the discovery of a major security weakness, the responsible representative of the tested organization will be informed and consulted on the further course of action.

6.6. Access data

A basic set of user permissions will be provided for testing purposes.

6.7. Communication scenario and test environment supervision

The test will be initiated by the tester with the explicit permission of the person in charge of the organization. This permission shall be given by the responsible person when the test performed according to this methodology cannot adversely affect the functioning of the organization

The organization actively monitors the systems and the corresponding part of the network infrastructure throughout the test.

In the event of an event affecting the operation of the system under test, the responsible person shall immediately inform the tester and, by mutual agreement, continue or terminate the test.

In the event of an event affecting a large number of systems, production systems or a significant part of the infrastructure, the responsible person shall inform the tester of the event and initiate the procedure according to the corresponding emergency plans. The tester shall immediately terminate the testing.

After the test is completed, the tester informs the person in charge that the test has been completed. The responsible person shall perform a system check. In the event of technical problems, he/she shall implement the appropriate contingency or recovery plan.

6.7.1. Risk of infection by malicious code

The test procedures do not pose a cyber risk (they do not carry malicious code) and therefore there is no need to take additional preparatory measures related to protection against malicious code prior to launch.

6.7.2. Risk of leakage of sensitive data

The handling of campaign data (user data such as name, surname, IP address, email, job title, final report) will strictly adhere to the principles of handling sensitive data, including GDPR regulations. The information obtained from the campaign will be removed during the testing process (e.g. the obtained passwords will not be stored in full, but only partially for reporting purposes, etc.). Exceptions will be defined and listed in this document.

6.7.3. Contact persons

Primary for client-side communication:

- will be determined before the test begins.

Contact person for communication on the supplier's side:

- **Daniel Přivratský, Service Manager (603 298 132)**

Next Generation Security Solutions s.r.o.

U Uranie 954/18, Prague 7, 170 00

sales@ngss.cz | www.ngss.cz

