SECURITY DAYS

ĮSILAUŽIMŲ TESTAVIMAS: AR GALIMA BŪTI ŽINGSNIU PRIEKYJE HAKERIO?

Vytautas Paulikas - Syntricks įkūrėjas, kibernetinio saugumo ekspertas
Lukas Apynis - Baltimax kibernetinio saugumo inžinierius, ESET ekspertas

Rugsėjo 5 d. 2024
KIBERNETINIO SAUGUMO KONFERENCIJA
esd.eset.lt

VERSLO ŽINIOS > TE

17:08

Prog
„Ign
duor

Lietuvos kariuomenė vasario 3-ąją fiksavo įtartiną prisijungimą prie kariuomenės nuotolinio mokymosi informacinės sistemos ILIAS naudotojo paskyros. Prorusiški programišiai skelbia įsilaužę ne tik į Lietuvos, bet ir į kitų NATO šalių karines sistemas.

ė

Publikuota: 2024-02

Programišiai nutekino 50.000 „Švaros brolių“

programišiai pardavinėja ir
brakulas.lt vartotojų duomenų
bazę: 257 tūkst. el. pašto
adresų ir slaptažodžių

Prorusiški programišiai įsilaužė į stebėjimo paslaugas vykdančios Lietuvos įmonės sistemą

Kokioms įmonėms aktualus įsilaužimų testavimas?

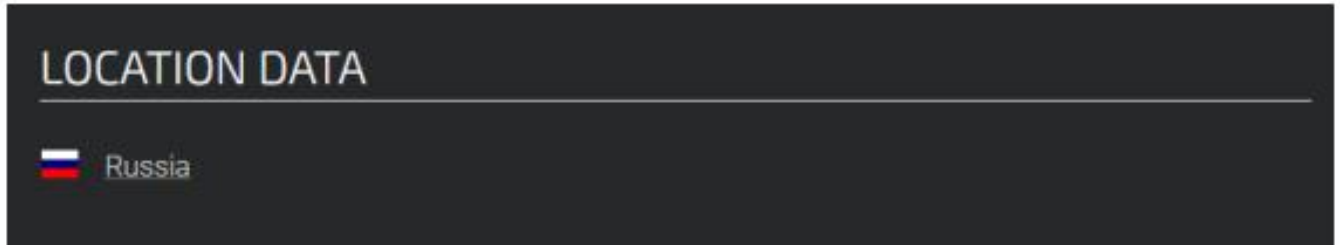
- **Teisinis reguliavimas** (**NIS2/TIS2**, PCI DSS, HIPAA, SOC 2 ir kiti)
- **Norite pamatyti:** išsamaus savo tinklo, informacinių sistemų ar interneto svetainių saugumo vaizdą
- **Norite suprasti:** ar programišiai gali pasinaudoti pažeidžiamumais ir kaip tai galėtų vykti
- Įvertinti **organizacijos darbuotojų** kibernetinio atsparumo įgūdžius

Incidentų tyrimai – blogos praktikos

Atakos pirminė informacija: atakuotojas kažkokiu būdu gavo RDP administratoriaus prisijungimus. Galėjo juos rasti nutekėjusioje DB, internete, arba naudojo „brute-force“ ataką, kad prisijungtų prie sistemų nuotoliniu būdu.

Sėkmingai prisijungė iš Rusijos IP per RDP su „Administrator“ paskyra.

-11 22:04:16.228	Security Logs	" " failed to log in (for a shared resource). ( )
-11 22:04:15.357	Security Logs	"Administrator" logged in via RDP. (W: S1, IP: (Russia), P: User32)
-11 22:04:15.357	Successful Rmt Logins	"Administrator" logged in via RDP from IP (Russia).



- Ataka įvyko vidurnaktį: 00:27 ir kiti, panašūs blokavimo laikai.

- **Atakos vidurnaktį: 00:27**
- **Atakos laikas: 22:04**
- **Atakos laikas: 20:00**

Saugumo problemos – nesaugi tinklo konfigūracija, RDP prisijungimas ir „Administrator“ paskyros slaptažodžiai:

Kaip vyksta įsilaužimų testavimas?

Penetration Test		Red Teaming
Gain oversight of vulnerabilities	**Goal**	Test the resilience against realistic attacks
Predefined subset	**Scope**	Realistic access paths
Focus on preventive controls	**Tested controls**	Focus on detection and response
Focus on efficiency	**Test method**	Focus on realistic simulation
Mapping, scanning and exploiting	**Test techniques**	Tactics, Techniques and Procedures (TTPs)
Very limited	**Post-exploitation**	Extensive focus on critical assets/functions
Parts of development lifecycle	**Recurrence**	Periodical exercise

Kaip vyksta įsilaužimų testavimas?

- **Darbų apimtis ir įžanga**
  - Darbų apimtis (scoping) – prieš pasirašant sutartį
  - Įžanga (kickoff) – prieš pat darbų pradžią
- **Žingsniai**
  - Informacijos surinkimas (information gathering)
  - Pažeidžiamumų paieška (vulnerability discovery)
  - Pažeidžiamumų patikrinimas ir išnaudojimas (verification and exploitaiton)
  - Dokumentavimas (reporting)
- **Rezultatų pristatymas**

Kaip vyksta įsilaužimų testavimas?

- **Įvadas**
  - Apžvalga
  - Darbų apimtis
  - Saugumo spragų santrauka
  - Papildomos rekomendacijos
- **Metodologija**
  - Naudota metodika
  - Rizikos apskaičiavimas
- **Techninė dalis** (informacija apie spragas ir individualios rekomendacijos)

A black-box penetration test of ServerX system was performed upon a request of CompanyZ. The purpose of the test was to assess the security of the target server. During the course of the audit a wide range of controlled attacks were performed. As a result of this test, multiple security vulnerabilities were identified.

Most of the identified security vulnerabilities arise due to outdated software, insecure configuration or improper user input filtering. By exploiting the identified issues a remote attacker could fully compromise the target system in multiple ways:

1. An existing Remote Command Execution (see page 28) vulnerability could be leveraged by an unauthenticated attacker to gain initial foothold and fully compromise the target by escalating privileges via outdated Linux Kernel software;
2. Multiple less severe vulnerabilities (see pages 15, 17, 21, 23 and 25) could be chained together to obtain administrative account credentials of the WordPress web application. Then, the theme or plugin editing functionality can be misused to gain limited remote command execution which would eventually lead to a privilege escalation and full compromise of the target system.

Due to severity of some vulnerabilities it is advised to take immediate actions to mitigate the business risks for CompanyZ. Most of the vulnerabilities can be easily fixed by updating the outdate software or performing minimal configuration changes. Remaining vulnerabilities require minor changes in the affected code.

Scope

The primary target of this audit was the ServerX system deployed in a test environment. The target was accessible via the following IP on the internal network to which a VPN tunnel was provided:

- 192.168.0.249 (serverx.host)

The audit was performed between 1st and 5th of January, 2023. Due to the nature of the audit (black-box) no user accounts were provided for the test.

Summary of Findings

The following table summarizes the identified vulnerabilities. An in-depth analysis of these findings is provided in the chapter ServerX (192.168.0.249) on page 7.

Table 1: Identified vulnerabilities

ID	Name	Risk Level
001	Clear Text Transmission of Sensitive Information	Low
002	Information Disclosure	Medium
003	User Enumeration	Medium
004	Persistent Cross-Site Scripting	Medium
005	Missing Anti Brute-Force Protection	Medium
006	Weak Password Policy	Medium
007	SQL Injection	High
008	Remote Command Execution	Critical

General Recommendations

It is not sufficient to solely fix the reported issues in order to increase the security of the IT infrastructure. Therefore, we provide additional recommendations which could help to minimize the risks of potential data-breaches.

1. Recheck. After the reported issues are resolved we suggest performing a recheck to ensure that the mitigations which were applied are appropriate. The recheck usually requires up to one third of the initial effort.

2. White-box audit. During a limited amount of time we covered only as much of the IT infrastructure as we could. While it was sufficient to assess the current state of the environment on a high level, some blind spots are remaining. We recommend performing a white-box audit at least on the most critical systems.

3. Periodic audits. New security vulnerabilities are discovered on a daily basis. Therefore, the software used across the IT infrastructure requires constant monitoring and auditing. We recommend to perform at least annual full-scale audits to ensure the security of the systems involved in providing services for the clients.

1. Black-Box

This approach tries to simulate a real world scenario in a way that the auditor, similarly to an external attacker, has no prior knowledge about the target. Usually, the auditor is only provided with an IP address(es) or a URL(s) of the target. In such a case, the pentester tries to figure out all the technical details about the target by extensive fingerprinting and information gathering and only then performs the actual test. While this approach is similar to a real-world attack, it is usually time-inefficient and cost-ineffective, because a real attacker is not limited in time.

2. Grey-Box

A grey-box approach allows the auditor to have partial insights into the target's infrastructure, used technologies, etc. For example, a network diagram, test users, partial documentation and other information is usually provided during such a penetration test. This information greatly speeds up initial stages of the audit and gives the auditor an opportunity to focus on the most important aspects of the audit.

3. White-Box

During a white-box audit a pentester has full knowledge about the target. This includes extensive documentation, test users, access to source code and underlying systems (via SSH, RDP or other means), close cooperation with IT team who maintains the target software/system, etc. This approach increases the likelihood of discovering vulnerabilities which are deep inside the code or require specific circumstances to exist for a successful exploitation.

Risk Calculation

The risk score in this report is based on the **Base Metric Group** of the Common Vulnerability Scoring System (CVSSv3). CVSS system allows easy comparison and risk assessment of identified issues as this system is widely adopted in vulnerability scanners and vulnerability databases. Once the risk score is calculated it is then transformed into a literal risk as shown in the table below.

Table 2: CVSS risk conversion

CVSSv3 Score	Literal
0.0	None
0.1 – 3.9	Low
4.0 – 6.9	Medium
7.0 – 8.9	High
9.0 – 10.0	Critical

005 Missing Anti Brute-Force Protection

Severity	Medium
CVSS v3	6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

Description

Multiple services running on the target server fail to limit excessive login attempts. As a result an unauthenticated attacker can perform brute-force attacks in order to gain access to user accounts having weak passwords.

Proof of Concept

During the audit it was identified that WordPress login form is not protected against a brute-force attack. Due to this issue, a quick brute-force attack using Hydra (https://github.com/vanhauser-thc/thc-hydra) was performed against the previously enumerated users (see chapter 003 User Enumeration).

```
root@kali:~# hydra -L /tmp/wp_users -e nsr serverx.host http-form-post '/wp-login.php:log=^USER^&pwd=^P
ASS^:S=Location'
Hydra v8.5 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations,
or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-08-24 22:21:31
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:4/p:3), ~1 try per task
[DATA] attacking service http-post-form on port 80
[DATA] with additional data /wp-login.php:log=^USER^&pwd=^PASS^:S=Location
[80][http-post-form] host: serverx.host   login: john   password: john
[80][http-post-form] host: serverx.host   login: tmartin   password: nitramt
1 of 1 target successfully completed, 2 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-08-24 22:21:35
```

Figure 15: Brute-force attack against WordPress login form

Similarly, a brute-force attack was performed against FTP service which resulted in a discovery of a valid credential pair.

```
root@kali:~# hydra -L /tmp/wp_users -e nsr ftp://serverx.host -t 2
Hydra v8.5 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations,
or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-08-24 22:22:10
[DATA] max 2 tasks per 1 server, overall 2 tasks, 12 login tries (l:4/p:3), ~6 tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: serverx.host   login: tmartin   password: nitramt
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-08-24 22:22:48
```

Figure 16: Brute-force attack against FTP service

Recommendation

We recommend to implement a secure CAPTCHA ("Completely Automated Public Turing test to Tell Computers and Humans Apart") security mechanism to protect against brute-force attacks against the WordPress web application. This can done by installing additional plugins or manually introducing the functionality. It is also recommended to limit the access to administrative parts of WordPress via ACL. For example, the following directives can be used in an `.htaccess` file placed in `wp-admin` folder to limit access by IP:

```
# Block access to wp-admin.
order deny,allow
allow from 127.0.0.1
deny from all
```

The FTP service can be configured to limit concurrent connections in combination with a fail2ban module which mitigates brute-force attacks.

More information can be found at:

```
https://wordpress.org/plugins/google-captcha/
https://codex.wordpress.org/Brute_Force_Attacks
https://github.com/fail2ban/fail2ban
```

Kaip išsirinkti paslaugų tiekėją?

- Pasikalbėkite su draugais ir kolegomis
- Atlikite rinkos tyrimą
- Paklauskite paslaugų tiekėjo kas įskaičiuota ir kaip vyksta procesas
- Paprašykite pavyzdinės ataskaitos
- Užklauskite kas konkrečiai atliks auditą
- Atsargiai vertinkite specialistų sertifikatus ir jų skaičių

Pabaigai

- Domėkitės kibernetiniais įsilaužimais ir jų testavimu
- Plėskite savo IT saugumo kontaktų ryšių sąrašą (jo prireiks)
- Jei nežinote, ar Jūsų įmonę galima nulaužti, pasibandykite
- Sekite NKSC veiklą ir naujienas (https://www.nksc.lt/)