Bypassing 2-Factor-Authentication via Voicemail Exploitation

7 messages

Shubham Shah <@gmail.com> Wed, Apr 30, 2014 at 4:15 AM
To: security@linkedin.com

-----BEGIN PGP MESSAGE-----
Version: Mailvelope v0.8.1
Comment: Email security by Mailvelope - http://www.mailvelope.com

wcBMA5t0URY+aVumAQf+M2tt/qsyAlRMzDtYoTyllNarUP8dMiCbAQLAWkQX
x4eO4ZUENdoT4aWbglSSIePc63CX5Alh+i13FZJl+M3SKfwh/r4CsfE6MQfq
ZR0MMAS1moXFHVkwb8r5Gk0n2iOpy5vUSr4d0JsQmEbuX/zlA6tARJqDcRE+
0ohR0TckIpb6BtLbCRqbAUj7ENdl/+Uara5MKZ92MHs9FNZkQRAJtw194wSK
RNtEX2gcDzAMaoZV05G0iWPawvFlxluzTYqVdUNfJFJ07VcqFlHzF9omShgO
db0ubgcjzNhFX8ucjRUKLAPN7LAOv2ULBs/xmtTAeAWA/KR7em5GT8NcU9S3
QtLlgAEfr9UJbt/hCZZaT4LW/mltLQbUkXprrAU/2Ds3OMXJkuNsh9plHj+s
J0Gd9ZeF6AQrVg5qpm+gfhM++2i11cbXUlWY6e690KcAl42LcdFlqzlZ+zG6
h5bsJAuE2NxRH+/XXwHdFcE2YBd49QpRwFH6rcPBqWKRWWXQNUdidybVEMev
FO7mkUoTWWtTZwwbtVqRVej8b4nPfA7VMZRZSLe3Z7toLq/KfG8Zgi+3fUvz
BV0QsOeVNJ24+962PQlqeV9bjkLYXM1i/TYPiPF53a0wdXTglu1pk9heMj9k
/5qvOltU8pmnco49O5qwfzEGPNaMgwSUXAi8y9TKqvrokuk55a2g+zkvD8NR
ONkA0U+E0/JSol6ebp9Cu08k58brq8eenx33jnr+LHPyWitkbQ4JOtYrYOd5
sO6BOBCQGKbr9Y3r1TpzyqtMiniZZve+gsGClSQa5a1Vq8Fya7/oWggogfl3
b73cCgnf2h0sDJjsn0gWUr+tqkCrBfRdyh39jcyimyr27P98KpaQRDaxZzyK
gYBBG3eaYNVYNPhrCyJJnKjLk8iWCThumf8y2BkNL9tF/pjFR3WvbTLzNiiB
mpRK3OxjBJA3qmgs8knG9YVVumVMqSTnElesTaS+GS0s8kgVFxzLU4lLxQ8D
Ek1/aSSykBgRtW9AwqrNKI22WJXTxkelzmzz6nWfvYQakuW6SGmPr1nGpFbK
o7OryJA0ydKVUAskNwOTM3EKc3FLIZJsh47kw1UaHlRVAXd4Md+glaD9DJdU
P2/xxLVxiK9fqkCA9lnOoF9dNQmyn7lNoYLdCGLZHzNM1clfb7n2v+s2Rk6d
X4Y5YU2ol6og4l1xk0aiB8VT3zS1L6gB9thiB7T53SzLpl77QbB1hHLkZ+5T
rKATQ0yVSqj3Ynzin0NbX9plQeGLlytoibCv/WlJLcdBKlwFCe25CcvADKUS
rA0amdp0cSO0JH8MuxqPTDPl7D9d7lPZF2UgZwvklOp2OA8T5OQEZG1nBIAw
88HVU0QWy33eSp/iXm2UtQgFqFdzMFaX7wTt2EL4Gv94hkkbcoi30FiBOqQ/
FmFHxhk+Bj9bHOWWm6XndEXYCb3XHa6RAe/IGlAvE8AKiRAaTjWJjWsXMgKC
CJ3AGDZMkzJUktOuelsNipv2rKoLS1lxtvsbh8hPql6Sidg1eZc4Kg5l4lOi
Lx7kYvq9HoQqshYFNNAlgz4VWBkVVZAXhBZ1qajWzsYIBFgE3Hr7mxI6EiDg
osRrk0W+Am3cJqRFVUmCwKc4lMsb8GyVlteIA5U0n4tTSnUKcBHp/RVT5GW0
FEYk2bptXlX9q0assssETnepTgoBNSBCJAVBjC8+dFrLtBZ8TmodfrKFbbxKv
8oS2hAQRJpFwY4IQ+Kh5nA/0F1+dyKwWB8RkwzsNW0ObUm4/d2pNa+Uf9lVa
RC/F3maob826a9rsBUGGpPs3axsPaSKygMW0unCdAGJHEAGvLCoxAsBZU7AT
4FLNBvoR2gvYxgXfbiHWJVTut7HRLEVhAKGKL/zeG0KyfRXpL0opLcLbiLgd
p6f1YvPcFP1eOiyykJ1Q09AnJoX9hChZE++YEdRHMGGdxGwxkbcKohlIB5FY
/DxVPlrucCWBumWYBLDQbHJr0AGgQjDlN1t2hblo9p0tU6Wn3XL01sLW9mtR
WCwlAJqWGDOmzruB0mpfoU+7MqsRxxzUlBirZ+u82RumFvl7WaPfogYqoDzI
3gwRKj4VP6R0KLb8zSc1+jMK74vLEnLtrq53fk6R5JlXwxn+DYaUpzos0fb8
xaXOw+JQfXliDiAEkzJwMLlRQzqZ0ZokcBYTkejADVZErWV9gQqNR8xkfOl/
cYAX6O9AU9848nCjvBV3Jrig8sH0iQnp/0JD1SDYlCokIguOlmSl/DxjupU6
dFXSomH/GT6UWPT99pQBdTJlg0B+2WXxB+oQ+KNcRqGTqKz/LB7liBJLN3/K
9qvtLVOyOYKGbht7+E3sO7C/VDXzDj2MqwxyE+uXl/zWcGYlhw8Gx/oaQb+c
pk/bysqawsPXiBgDfZBEXki7XqgSmrwPWNit2WtwyPbJcMxWOCWtKiawQl7X
1zh/vbj9MPYKyr8fvUxWEKyalgVffeSRf9cjlKajb4A2AyoaGBj8v3iMRZO8
ZYIZE/cRNY1xQESUbrLERzJuXu9JaRcdbqURMCAzVY0BcY2cTEH/Qww4lPok
G8e3Z0NYP31hVRl04SLoHF1CBrTHldo156AwUM+qLB3X4QrkA1AwrOjfL0z
yV0Z7jxsxWlmmaz4go+QdWd5Ycgut5MzKvx6fx4emJ9ZLlrENdPDyo26kwnn

yz1agFNbJDoMP3oqKH4WBOi8DKk+XdQqiv02M+MBP6w1OnqTOavUeBmbiF/O
4Idv237iThJ88EdwwTvnip+ro3arZVmZd8tLAv51uhFBVmpVwGzJRpwHOaLc
BB9DTORNfrJX0yLvgUn+CfJl4DmNMxPODUSFMzjbO0mIidHoppmxVnhz9QAn
BCFInuist+ceyDKrwVbLwBF/2weMd0BXA95uMBhH7yJPKZSIzFWgAWH7yTca
Zi5kbybscM0k2VyuTaADEaQV/zqCGUsuBIoc1jbR+uCCcyLRcTYMEWu2bl6F
I+jxgx6Oe9yFkAhvEpquXrVoPV/i6JSCgR8+7/xWnAnOGGhcNHQE1L/FRJcv
G6Y/VZ67M0RxdJDoziHsBOfas9tIELiawfBjIt5F2Mnj/jVJgkzblGeof0d9
tk+C6d2g3TGP5GP7DMwY2TWnS0pi67fpPtDw2rSR8AoCmXX2jsh42zDomEIH
lPxKIFKGMtEsVvlmuOD72ZGiyF60UuEp80iyyDTe7FW7AJvTKMw+96H9Gj1
0LeVxYo6AneqTa+k9F1/KrEsIG1TpuSbROQglvH6bJuob/hQp2mRdEsIFkPn
5TxlQU2U/HZVZcYnS7uGHGlnwA2g/Tn9rrpGN+NwE4D3C72ObJX5kwvl0Uuo
fNvhH+UkUpldN0TEhd4BAWsdOh+q42YGPiNX0F2GtGCpr1v14GSjBtm0K1lK
SCLgl6KnSrlk/wjq+QwaxVqh5Z64Lsmo6zLUOalEUgM2rlv/43cnLDjb9A6M
uyMyrwlAnFuvMh19LuMIL22yUHkKucQiK89cMXQDwcg=
=XAQ5
-----END PGP MESSAGE-----

Clint Ruoho <cruoho@linkedin.com> Wed, Apr 30, 2014 at 4:51 AM
To: Shubham Shah <@gmail.com>

Hi Shubham,

Thank you for your report. We will investigate it and get a response back to you when we have completed our analysis.

Thanks,
Clint
--

Clint Ruoho
Sr. Information Security Engineer
House Security

LinkedIn

cruoho@linkedin.com
linkedin.com/in/clintruoho

From: Shubham Shah <>
Date: Tuesday, April 29, 2014 at 11:15 AM
To: security <security@linkedin.com>
Subject: Bypassing 2-Factor-Authentication via Voicemail Exploitation
[Quoted text hidden]

Shubham Shah <@gmail.com> Sun, May 4, 2014 at 4:39 PM
To: Clint Ruoho <cruoho@linkedin.com>

Hi there,

I have disclosed the bug to Optus (Telco) on the 2nd of May. In accordance with Google's vulnerability disclosure suggestions, the bug related to the telco's as well as the disclosure stating the possibility of bypassing 2FA will be disclosed publicly within 7 days.

I hope that Optus fixes the issue within 7 days, so that when we publicly disclose, Australian's are safe from the 2FA bypass I disclosed to you. However, if Optus does not fix this issue within due time, a public disclosure with the details of bypassing 2FA auth will be released.

From further research, I believe that the voicemail vulnerability is actively known and exploited in the wild, and hence believe it's necessary to continue with disclosure.

Hopefully, before the due date for disclosure, LinkedIn is able to reply to this information.

[Quoted text hidden]

David Cintz <dcintz@linkedin.com> Fri, May 9, 2014 at 5:55 AM
To: Shubham Shah <@gmail.com>

Hi Shubham,

Thank you for notifying us of this issue before publicly disclosing it.

While the potential impact for our members is limited, we have made the decision to temporality turn off the voice option in our Two-Step verification setting. We are working with the third-party vendor we use for this service to implement a fix. After the fix is in place, we will evaluate turning the voice option back on.

Also, would you mind sharing how do you plan on disclosing this?

Thanks,
David

David Cintz
Technical Program Manager, Security Ecosystem
House Security

LinkedIn

dcintz@linkedin.com
linkedin.com/in/dcintz

From: Clint Ruoho <cruoho@linkedin.com>
Date: Tuesday, April 29, 2014 at 11:51 AM
To: Shubham Shah <>
Subject: Re: Bypassing 2-Factor-Authentication via Voicemail Exploitation
[Quoted text hidden]