From: "cisco-data-incident@cisco.com" <cisco-data-incident@cisco.com>
To: EMAIL ADDRESS
Subject: NOTICE OF DATA BREACH

NAME
ADDRESS
ADDRESS

November 2, 2016

Dear NAME:

WHAT HAPPENED
As part of Cisco's commitment to trust and transparency, we are writing to inform you about a situation which may affect you.

An independent security researcher discovered that a limited set of job application related information from the Cisco Professional Careers mobile website was accessible (https://mjobs.cisco.com). Cisco's investigation found this to be the result of an incorrect security setting following system maintenance on a third party's website. Upon learning this, the setting was immediately corrected and user passwords to the site were reset. Because Cisco takes its responsibility to protect information seriously, and since many people use the same passwords on multiple websites, we wanted to alert you.

As a precaution, as a user of the Cisco Professional Careers Website, you will need to reset your password at their next login by clicking "forgot my password".

WHAT INFORMATION WAS INVOLVED
The security researcher was able to access information which included the following data fields: name, address, email, phone number, username and password, answers to security questions, education and professional profile, cover letter and resume text, and voluntary information (if entered) such as gender, race, veteran status, and disability.

Our combined investigation discovered that the incorrect settings were in place twice. The first time was from August 2015 to September 2015, and the second was from July 2016 to August 2016. At this time, based on our investigation, we do not believe that this information was accessed by anyone beyond the researcher who found and reported the issue. However, we are taking precautionary steps.

WHAT YOU CAN DO
Beyond the required password reset, we recommend that you update/change your login credentials, password and security questions / answers for any other websites that use the same credentials and information as the Cisco Professional Careers mobile website.

Additional Options:
Obtain More Information to Protect Yourself

Visit any of the three US Credit Bureau websites for general information regarding protecting your identity. And the Federal Trade Commission has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

Place a 90-Day Fraud Alert on Your Credit file
An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Order Your Free Annual Credit Reports
Visit www.annualcreditreport.com or call 877-322-8228.
Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Manage your personal information
Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

Use Tools from Credit Providers
Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity.   If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

FOR MORE INFORMATION
Cisco has established an incident response page where you can find the most current information related to this incident:
http://www.cisco.com/c/en/us/about/security-center/sto-alerts/2016-security-announce-professional-careers.html

If you have further questions, or would like help from a Cisco representative, please contact Cisco's data incident response team at cisco-data-incident@cisco.com or +1 408 526 8888 (select option 3 then option 1).

For more information on obtaining free credit reports or identity theft protection:

Experian
Experian Security Assistance
P.O. Box 72
Allen, TX 75013
Phone: (888) 397-3742
Email: BusinessRecordsVictimAssistance@experian.com

Equifax
U.S. Consumer Services
Equifax Information Services, LLC.
Phone: (678)-795-7971
Email: businessrecordsecurity@equifax.com

TransUnion:
P.O. Box 6790
Fullerton, CA 92834
Phone: (800) 916-8800
Email: fvad@transunion.com

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Telephone: (202) 326-2222
(877)-FTC-HELP (382-4357)
Website: www.ftc.gov

Your State Attorney General's Office
California Attorney General
1300 I St., Ste. 1740
Sacramento, CA 95814
(916) 445-9555
Website: ag.ca.gov

Sincerely,
The Cisco Data Protection Team