Heartbleed Vulnerability Information

IT Status
Update 4/25/2014

[Change your passwords][1] by May 5th, 2014, as part of Virginia Tech’s response to the Heartbleed security issue.

The Virginia Tech Information Technology Security Office is requiring all users to change their PID, Oracle (Banner), and VT Google Apps passwords by May 5th, 2014.

Hokies (Exchange) passwords and Network passwords (password used for VT-Wireless and VPN) are not affected by this password change requirement.

Some services accessed through PID, Oracle (Banner), and VT Google Apps passwords were affected by a security flaw in OpenSSL encryption, discovered on April 7th, 2014. The Heartbleed vulnerability allows an attacker to remotely extract data including usernames and passwords from vulnerable Web servers without the user’s knowledge. The attack cannot be detected.

At Virginia Tech, all servers known to be vulnerable have been patched, and security certificates have been replaced. There has been no evidence that Virginia Tech data or systems have been accessed inappropriately as a result of the vulnerability. Because of the nature of the vulnerability, password changes will be required to reduce the possibility of any malicious access to Virginia Tech resources.

Users who changed their passwords on or after April 22nd, 2014 should not need to change them again. Any passwords changed before the 22nd of April WILL need to be changed again.

Users who have not changed these passwords by May 5th, 2014 will have to select a new password the next time they log into services requiring PID or Oracle (Banner) passwords.

Virginia Tech students, faculty, and staff are also urged to change passwords for all other outside web services affected by Heartbleed, including many social media, cloud computing, news, banking, and commerce sites. See the Heartbleed hit list at mashable.com [2] to view many of the popular internet services affected and the vendor security recommendations for those services. Users changing passwords for services outside the university should be sure NOT to reuse your Virginia Tech passwords. Be aware that phishing attempts increase during widely-publicized information security events. Keep in mind that no legitimate company or organization will ever ask you to give them your password via phone or email.

Changing passwords can be accomplished by following the instructions at Changing My Password [1].

If you have questions or difficulties with changing your passwords, please contact 4Help at (540)
Heartbleed Vulnerability Information
Published on Computing @ Virginia Tech (https://computing.vt.edu)

231-4357.

For more information on the Heartbleed vulnerability see the following:

- [The cartoon version of what Heartbleed does on XKCD.com](http://www.xkcd.com/1354/) [3]
- [The potential extent of the damage from Heartbleed on Arstechnica.com](http://arstechnica.com/security/2014/04/heartbleed-vulnerability-may-have-been-exploited-months-before-patch/) [4]
- [Slightly more technical info from Codenomicon on heartbleed.com](http://www.heartbleed.com/) [5]
- [Vendor notifications from the SANS Institute on isc.sans.edu](https://isc.sans.edu/forums/diary/Heartbleed+vendor+notifications/17929) [6]
- [List of external sites that recommend changing passwords on mashable.com](http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/) [2]

Service Info

Service Info [Resolved]

Created: Thu, 04/10/2014 - 1:52pm Resolved: Fri, 05/09/2014 - 1:20pm Duration: 4 weeks 23 hours 28 min 7077 Views

Source URL: [https://computing.vt.edu/content/heartbleed-vulnerability-information](https://computing.vt.edu/content/heartbleed-vulnerability-information)

Links:
[1] https://computing.vt.edu/kb/entry/3924