VoiceThread in Wayland Public Schools

A very vulnerable foundation puts our student data at risk

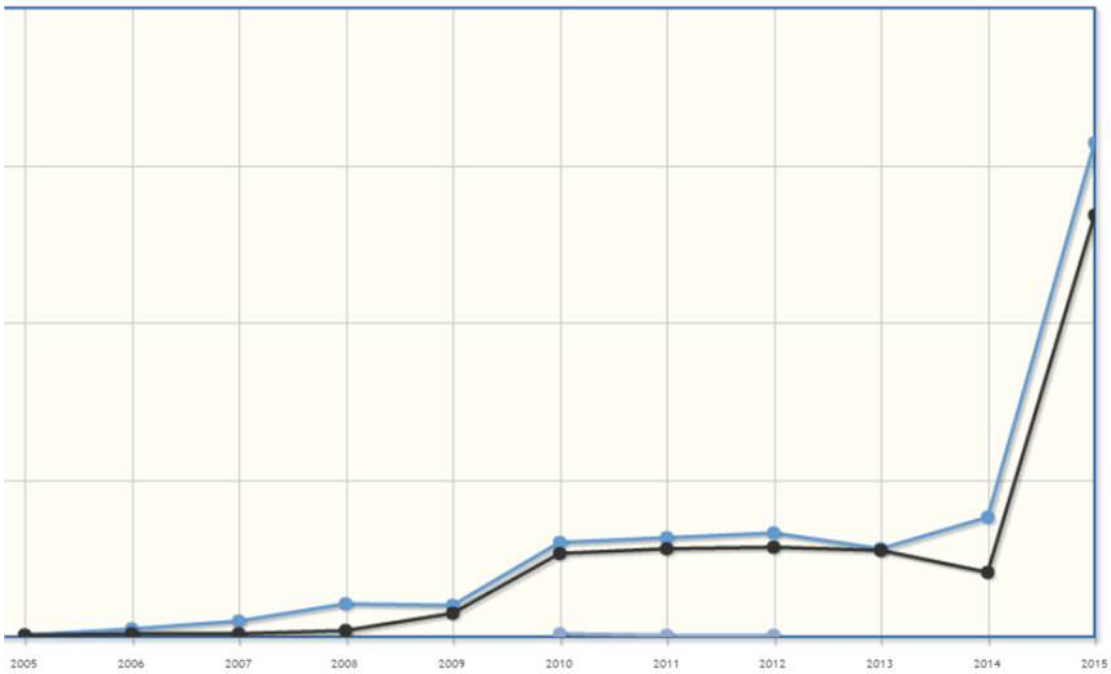
Wayland Public Schools is using "VoiceThread", a Web-based system to record interviews and presentations. According to their website, "VoiceThread is a cloud application, so there is no software to install. The only system requirement is an up-to-date version of Adobe Flash." *See:* https://voicethread.com/about/features/

This makes VoiceThread a very risky platform for Wayland Schools. Adobe Flash has been one of the most vulnerable and insecure applications worldwide, year after year. In December of 2015, for example, these were some of vulnerabilities that were found:

#	CVE ID	Vulnerability Type(s)	Update Date	Score	Access	Complexity
1	CVE-2015-8651	Exec Code Overflow	12/29/2015	9.3	Remote	Medium
	Integer overflow in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors.					
2	CVE-2015-8650	Exec Code	12/29/2015	9.3	Remote	Medium
	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, and CVE-2015-8649.					
3	CVE-2015-8649	Exec Code	12/29/2015	9.3	Remote	Medium
	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, and CVE-2015-8650.					
4	CVE-2015-8648	Exec Code	12/29/2015	9.3	Remote	Medium
	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8649, and CVE-2015-8650.					
5	CVE-2015-8647	Exec Code	12/29/2015	9.3	Remote	Medium
	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.					
6	CVE-2015-8646	Exec Code	12/29/2015	9.3	Remote	Medium
	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.					
7	CVE-2015-8645	DoS Exec Code Overflow Mem. Corr.	12/29/2015	9.3	Remote	Medium
	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8459, CVE-2015-8460, and CVE-2015-8636.					
8	CVE-2015-8644	Exec Code	12/29/2015	9.3	Remote	Medium
	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion."					
9	CVE-2015-8643	Exec Code	12/29/2015	9.3	Remote	Medium
	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.					

Note that this is the list for *only one month* and <u>all</u> of the CVSS scores are above >9 on a scale of 1 (lowest risk) to 10 (highest risk). A copy of this spreadsheet is attached.

The number of Flash vulnerabilities also jumped in 2015:



Every WPS computer is vulnerable to Flash defects

Flash vulnerabilities affect every type of computer that WPS uses: Mac, Windows and Chromebook. With 'zero day' exploits, Flash is a major problem in any organization. For Wayland Schools, with repeated delays in patch installation, Flash is a data breach waiting to happen. A copy of Adobe's latest patch alert is attached.

Problems with VoiceThread's approach:

- **XSS vulnerabilities:** VoiceThread's website states: "VoiceThread's primary application platform is currently Adobe Flash, which is inherently not vulnerable to XSS attacks." This claim not accurate. See the attached document that lists Flash XSS vulnerabilities from 2006 through 2014.
  See: https://voicethread.com/howto/common-security-vulnerabilities/

- **No encryption for user data:** The same page states, "... as user data is not encrypted." If student voice and video recordings are never encrypted, at rest or during transfer over the internet, this creates a major risk for users.

- **SSL "option":** The same page state, "If an organization chooses to enable SSL by default, then all content other than inbound audio and video recording is protected using SSL, including cookies, session data, and related content." This is another puzzling choice; all VoiceThread sessions, inbound and outbound, should be protected by strong SSL encryption by default to protect their clients. This is similar to standard SSL protection included on every major Web shopping site.

Conclusions:

1. **Wayland Public Schools teachers should be notified immediately**; VoiceThread should be banned as an application recommended or used by WPS staff.

2. **This is a good example of the need for review and approval by WPS** before Web-based or installed software applications are used by WPS teachers or staff. Every app must be thoroughly reviewed, and a data security agreement must be signed with each Web vendor as recommended by the US Department of Education. If a breach occurs, WPS will be responsible and Wayland taxpayers will foot the bill. Wayland student and family data will be lost, forever.

3. **Wayland Public Schools needs a clear, written policy** regarding the use of new Web and installed software applications, or this problem will recur.

4. **Wayland parents should have the opportunity to review and approve / deny** the use of each Web or installed application, to protect our privacy and security.

Mark Hays
Wayland Computer Privacy Initiative