Unsealing the Halderman report would be Responsible Vulnerability Disclosure

Statement by Computer Security Experts, May 11, 2023

The report on security flaws in Dominion voting machines, written by Professors J. Alex Halderman and Drew Springall in July 2021 and placed under seal by the Federal District Court for the Northern District of Georgia, should be immediately unsealed by the Court and be made public. It is widely recognized by computer security experts in both industry and academia that keeping vulnerability details secret, *past* the time in which a vendor could reasonably have patched them and indeed past the time in which the vendor *has* patched them, harms the security of users.

Bugs in computer software can be *exploitable vulnerabilities*, meaning that hackers who know about these bugs can exploit them to take unauthorized actions. When such bugs persist without being fixed ("patched" in the language of computer security) and without the distribution of software updates incorporating such fixes, then users of such software suffer harms due to the insecure software. Today, it is uniformly recognized that keeping vulnerabilities secret does not provide security. If someone can discover a vulnerability, others can as well.

In the early decades of computer systems, vendors were very slow to patch systems. To address this problem, a system of *responsible disclosure* was developed in the late 1990s and early 2000s, and this system is now widely accepted by industry (both the vendors and users of software), government agencies such as CISA, and by security researchers world-wide.

Upon discovering a security flaw, a security researcher practicing responsible disclosure will notify the maker (either directly or via one of the organizations that exists for this purpose) of all the details needed to understand and reproduce the problem. The researcher will inform the maker that after a set period (generally around 90 days) all the details will be published.

The purpose of the (delayed) public disclosure is twofold:

1. to incentivize software vendors to fix their bugs and distribute those fixes promptly (or to produce less buggy software in the first place);
2. to inform consumers of software so that they may improve their own security, either by installing such fixes or by discontinuing the use of vulnerable software.

This process–early notification to vendors followed by public disclosure–is the industry norm. Corporate CSOs (Chief Security Officers) who are *consumers* of commercial software rely on public notification to secure their own businesses. Makers of software (at sufficiently high level of professionalism) are well organized enough to act upon vulnerabilities disclosed to them. Google's "Project Zero" is a team of security researchers that have released 1791 disclosures after a 90-day delay, and 6 disclosures on which they delayed release for not more than 216 days.[1] An entire industry exists to assist companies in paying cash bounties to independent researchers who responsibly disclose bugs and vulnerabilities.[2]

Before responsible disclosure became the norm, vendors would ignore security flaws; before (delayed) full disclosure of details became the norm, vendors would claim that the flaws were merely "theoretical."[3] They would leave their systems vulnerable – sometimes taking years to patch their software, or never patch their software – relying on the ignorance of their customers.

Those who argue that publishing vulnerabilities enables bad people to do bad things, are ignoring the fact that if one person can discover a flaw, so can others. This is why responsible disclosure, including the follow-up of full disclosure, is so widely practiced and accepted in the computer and software industry. In this particular case, the report in question has been widely distributed *with and without* authorization.[4] Bad actors undoubtedly already have access to the report. There is further danger that it could leak to the general public at any time. A leak close to November 2024 could be used as a political tool to undermine confidence in the election.

We have not read Professor Halderman's report, since it is still under seal, but (from all descriptions of it) it is a classic example of a security-vulnerability report that should now be released to the public. The report has been available to the vendor for over 500 days, so there has been ample time to patch those vulnerabilities that *can* be patched. In fact, Dominion claims to have fixed some vulnerabilities apparently related to the Halderman report, in their Democracy Suite 5.17 product, according to their recent filing with the EAC.[5]

Today, the customers of Dominion's product—election administrators, public officials, and *voters*—need full information about its security so they can make their own fully informed judgments about how to run their elections. Citizens can ask their state election officials to *install* Dominion's update rather than leaving it on the shelf.

[1] https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html, accessed May 9, 2023.

[2] HackerOne https://hackerone.com/bug-bounty-programs (accessed May 9, 2023) links to hundreds of such bug-bounty programs, and in many of these the terms of service permit the bug reporter to unilaterally go public after a specified number of days.

[3] Schneier: Full Disclosure of Security Vulnerabilities a 'Damned Good Idea', by Bruce Schneier, in *CSO Online* magazine, January 9, 2007. https://www.csoonline.com/article/2121803/schneier--full-disclosure-of-security-vulnerabilities-a--damned-good-idea-.html or https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html

[4] In addition to the real possibility of independent discovery, it is also the case that dozens of people have read the Halderman report (with authorization): legal teams from the Defendants in this case, legal teams on both sides of the Dominion v. Fox News lawsuit, employees of US CISA and EAC; and MITRE got it from Dominion without the Court's authorization.

[5] https://www.eac.gov/sites/default/files/voting_system/files/D-Suite%205.17%20Certificate%20and%20Scope%20SIGNED.pdf

Since Professor Halderman wrote his report pursuant to the Court's Protective Order, the decision is not his to make: it is now up to the Court to practice responsible disclosure by unsealing the report. We urge the Court to do so immediately.

Signed,

Andrew W. Appel, *Eugene Higgins Professor of Computer Science, Princeton University*
Bruce Schneier, *security technologist and Lecturer at the Harvard Kennedy School*
Prateek Mittal, *Professor of Electrical and Computer Engineering, Princeton University*
David L. Dill, *Donald E. Knuth Professor in the School of Engineering, Emeritus, Stanford Univ.*
Vanessa Teague, *CEO, Thinking Cybersecurity Pty. Ltd. and Associate Professor (Adj.), the Australian National University*
David Jefferson, *Computer Scientist, Lawrence Livermore National Laboratory (retired)*
Poorvi L. Vora, *Professor of Computer Science, The George Washington University*
David Naumann, *Professor of Computer Science, Stevens Institute of Technology*
Duncan Buell, *Chair Emeritus — NCR Chair in Computer Sci. and Engineering, U. South Carolina*
David Wagner, *Professor of Computer Science, University of California, Berkeley*
Ronald L. Rivest, *Institute Professor, Massachusetts Institute of Technology*
Patrick McDaniel, *Tsun-Ming Shih Professor of Computer Sciences, Univ. of Wisconsin-Madison*
Josh Aas, *Executive Director, Internet Security Research Group*
Douglas W. Jones, *Emeritus Associate Professor of Computer Science, University of Iowa*
Peter G. Neumann, *Chief Scientist, SRI International Computer Science Lab*

Affiliations are listed for identification purposes only and do not indicate endorsement by the institutions mentioned therein.