

VulnWatch: [VulnWatch] serious vulnerability present. all doomed. over.

[VulnWatch] serious vulnerability present. all doomed. over.

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-04/0003.html>

From: Security Experts, Liability Limited (throwaway@dione.ids.pl)
Date: 04/01/03

Date: Tue, 1 Apr 2003 04:39:25 +0200 (CEST)
From: "Security Experts, Liability Limited" <throwaway@dione.ids.pl>
To: Potential Customer Awareness Forum <full-disclosure@netsys.com>, Prospective Customer Resources

```
-----  
| S.E.L.L. -- ADVISORY NUMBER 4F4E45 -- .L.L.E.S |  
|-----|  
| April 1, 2003 |  
||  
| We totally deny the allegations, and we're |  
| trying to identify the allegators. |  
||  
-----
```

S.E.L.L. disclosure timeline:

01/05/99: vulnerability identified and tested by S.E.L.L.
01/06/99: S.E.L.L. customers notified
01/06/99: oh, and I told my wife, she said it's silly
05/15/99: we got our tester out on bail
12/20/02: still don't get any respect from wife
03/30/03: vendors notified
04/01/03: public disclosure

Synopsis and impact:

A distributed denial of service condition is present in the election system in many polypartisan democratic countries. A group of determined but unskilled and not equipped low-income individuals, usually between 0.05% and 2% of overall population of the country, can cause serious disruptions or even a complete downfall of the democratic system and its institutions, and wreak havoc and destruction without using any force.

This is considerably less than the majority of voters required in more conventional attacks, at least in this social group.

VulnWatch: [VulnWatch] serious vulnerability present. all doomed. over.

The attack is generally difficult to prevent once occurs, since it is not possible to make immediate changes to election ordinances, especially once the process have started. Changes are often required to be passed at least one year before taking any effect. As such, patching the bug might take a considerable amount of time, perhaps also sufficient for the country to fall into chaos and oblivion, and for things of unspeakable horror to happen to all people like you and me.

Our company supports and takes pride in responsible and accurate vulnerability reporting.

Not vulnerable:

- United States (but to be evaluated)
- Monarchies and dictatorships (until overthrown)
- International waters (until claimed)

Attack details:

The attack relies on the fact that numerous election ordinances require a certain number of voter signatures to be collected in order for a candidate or a party to enter elections and be placed on a national election list.

This approach is generally non-discriminatory, and it is impossible to deny the right to be included on such a list for an otherwise eligible individual who collected a given number of verifiable signatures. Most countries do not implement a regulation that requires all votes on all lists to be unique – so a single person can change his or her mind and support two candidates. This is because of the difficulty of cross-verification – most election procedures must still rely on manual checking – and the possibility of malicious action of a hostile voter, of course.

Depending on the election level – local, parliament or presidential – a different number of signatures has to be collected. The number is usually everywhere from 0.05% to 2% of the total population – typical figures are 1000–10000 (common for parliament), or 100000–1000000 (presidential) for a medium to large country of 10–50 million citizens.

In our example, we use parliament elections where the minimum is set at 10000. In order for the attack to be successful, the attacker would have to find that many co-conspirators – usually not impossible, since many voters are dissatisfied with the system or life in general, or can be bribed or tricked into signing a list. A careful attacker might choose a larger number of co-conspirators to decrease the chances of the attack being detected in routine signature validation phase. This could lead to all

[VulnWatch] serious vulnerability present. all doomed. over.

VulnWatch: [VulnWatch] serious vulnerability present. all doomed. over.

conspirators being charged on the grounds of conspiracy to overthrow the government – although charging all 10001+ conspirators might be an effective DDoS on the judiciary and penitentiary system of a mid-size country, so this measure might have very undesirable results anyway.

Every co-conspirator would have to make a small investment, buy a few pens and several sheets of paper, and put their name on only a single page of this stack. He would then have to bring his sheets to the central site.

Considering that one sheet of paper can hold approximately 300 names (use three columns of 50 and both sides of a sheet), the number of sheets required to collect all signatures would not exceed 33 per person. This might be slightly unrealistic, but even buying 100–200 pages is a minor expense.

We assume that a single person can take up to three hours of his everyday life on a daily basis to sign other people's lists, and that three hours are enough to place approximately 500 signatures. A single person can travel once every five days to the conspiracy HQ.

Of all 10001 pages that are signed, each person gets a set of 2500, which is 5 days worth of work, and also gets the stack of blank pages brought along with the signed one. Five days later, all persons stop by the central location, and pass their finished first pages, with signatures, to the next person, who passed his pages to the next person, etc. The last person passes to the first person, and, at this point, all people have 2500 new pages to put their names on.

This process continues. When a person gets a page that is full, he or she reaches to his blank page stack and staples it to the document, then puts his or her name on the list on this page.

Within approximately one month, all 10001 lists are full and cross-signed by all candidates (except by the candidate himself, this is why we need this one extra co-conspirator). With personal expenses of few bucks per conspirator, and with just weeks of mildly time-consuming work, this method can be hardly called time- or resource-consuming.

At this point, all conspirators can apply for being listed as a candidate, and cannot be denied this right. The outcome, should elections proceed – and there might be no grounds for cancellation – will be a logistic disaster. Completely unexpected, gigantic printing and distribution costs for phone book size ballots, utter confusion of many voters, troubles with storing and counting ballots – all pages of this book-ballot would have to be reviewed to make sure the vote is valid and only one candidate is checked...

The inability to proceed with elections due to lack of funds or resources for printing and distribution, or the inability to count ballots for weeks and months to come, might cause serious impact on the country and the democratic system (might not apply to Florida).

VulnWatch: [VulnWatch] serious vulnerability present. all doomed. over.

Fix:

Vendor parliaments can prevent this attack by establishing a convenient dictatorship or a monarchy, or becoming the 51th state. In the States, candidates outside the bipartisan system are usually listed just as a harmless prank, and would not be missed.

Fixes that implement cross-verification of signature uniqueness across lists are susceptible to another DoS condition and are generally not recommended.

Note: some countries impose serious penalties for a conspiracy to overthrow the political system. THIS DOES NOT FIX THE VULNERABILITY.

Security-by-stringent-consequences model is considered to be broken by design. Besides, there's another DDoS possibility if an attempt to jail all conspirators is being made, per our discussion above.

Our recommendation is for all countries to implement the first solution proposed. Note: subsequent implementators of the last option of the "state" option might find the number 51 already taken; please increase the number until a unused number is found. Be sure to avoid integer overflows - do not use 'char' for computations.

About S.E.L.L.:

S.E.L.L. is a number one provider of deep-insight security strategies for maximizing ROI with state-of-the-art TCO management customer-facing security philosophy. As a successful company in a competitive market, we strive to provide the complete solution for enhancing your B2B experience.

Founded in a garage in Latvia, we soon become the realization of the American Dream, growing to an extended family of 300. Then down to 15. Our customers include many.

Subscribe now for our future alerts - it's free. Sort of. Don't blink.
