Unisyn Vulnerability Disclosure Policy

Version 1.0 August 14, 2020

Introduction

Maintaining the security of our products is a high priority of Unisyn Voting Solutions (Unisyn). This Vulnerability Disclosure Policy (VDP) is intended to provide a clear channel for the security research community to provide vulnerability disclosures to the appropriate Unisyn staff.

This policy allows Unisyn to receive, assess, mitigate, and communicate about security vulnerability disclosures. Unisyn hopes that this formalized policy will foster an open dialogue with members of the security research community, because Unisyn recognizes that the work done by that community is important in continuing to ensure the security of our products.

This policy is also future facing and will serve to guide Unisyn as we expand and mature our vulnerability disclosure program to include voting system products.

The Election Infrastructure Special Interest Group (EI-SIG) white paper on this topic[1], recognizes that the effort to foster communications with the security research community will only be successful if it is accompanied by changes that streamline and modernize the broader elections infrastructure. Specifically, Unisyn encourages:

- Federal Elections Partners/EAC to develop a process to permit the rapid mitigation of critical vulnerabilities without negatively impacting the certifications of those systems.
- State and local elections officials to adopt processes to coordinate with the Federal certification process to allow mitigated systems to be rapidly deployed in election jurisdictions, as needed.
- Industry and Government to consider economic models that will assist local election officials with the cost and logistics of upgrading their technology on a regular basis.

To encourage responsible disclosure, Unisyn commits that if a vulnerability report is made in accordance applicable laws and with the guidelines set forth in this policy, Unisyn will not pursue legal action against the individual or entity providing the report.

[1] https://130760d6-684a-52ca-5172-0ea1f4aeebc3.filesusr.com/ugd/b8fa6c_2f2f6a876e3c4f56a44a13a537fd26e2.pdf

Scope

Unisyn's Vulnerability Disclosure Policy currently covers the following:

- Unisyn's public facing web site https://unisynvoting.com/

Over the coming months, Unisyn will be engaging with security researchers as part of the ongoing process to mature and expand our vulnerability disclosure program. We expect that this effort will lead to the development of a managed vulnerability disclosure program for one of our more modern voting systems.

Unisyn Guidelines for Responsible Disclosure

Unisyn requires anyone who is interested in researching and reporting security issues to observe these requirements of responsible disclosure.

- Please confirm that you are not on the U.S. Department of the Treasury's Specially Designated Nationals List.
- Do not engage in activities in connection with vulnerability research or testing that are in violation of any applicable national, state, or local law or regulation.
- Do no harm or damage to Unisyn, its representatives, its customers or election officials in research and testing Unisyn products.
- Report any security issue only to Unisyn and refrain from making information about the vulnerability public before expiration of a mutually agreed time frame.
- Provide full details of the security issue to Unisyn in a report and be open to describing how the vulnerability was found so Unisyn may reproduce the conditions.
- Provide well-written, detailed, and fact-based reports in English to Unisyn to make the tasks of understanding and mitigating the issue easier and quicker.
- Do not send reports that relate to Unisyn products that are out of scope under the current policy.
- Do not engage in testing or research that corrupts, permanently modifies, or deletes the data of Unisyn or Unisyn customers.
- Do not engage in research or testing activities that involve DDoS or other disruption, interruption, or degradation of internal or external systems or services of Unisyn, Unisyn dealers, local election officials or Unisyn customers.
- Do not wrongfully disclose or use confidential or proprietary information, or information that is subject to restrictions on disclosure or use under state or federal privacy laws.
- Do not engage in social engineering attacks, phishing emails or use other social engineering or deceptive practices or techniques against anyone, including Unisyn, its dealers, contractors, or election officials.

What you can expect from Unisyn:

- A timely response to your vulnerability report by email (within 5 business days).
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has been completed in each stage of our process (including certification at the U.S. Election Assistance Commission and/or by a State or States).
- An expected timeline for availability of patches and fixes.
- Public credit for discoveries and reporting the vulnerability after the vulnerability has been validated and mitigated by Unisyn for affected customers.

Unisyn does NOT offer monetary compensation for reporting vulnerabilities under this policy. Unisyn will, as noted above, give credit, and say thank you for new and useful vulnerability reports via email as well as publicly on our web site.

Report security vulnerabilities to:

security@unisynvoting.com

When submitting a report concerning a suspected vulnerability please be sure to include a valid email address where we can contact you should we require additional information.

Please note that your submission of a potential security vulnerability finding is voluntary and subject to the terms and conditions set forth in this policy. By submitting a vulnerability to us you acknowledge that you have read and agreed to this policy.

Unisyn may modify the terms of this policy or terminate the policy at any time.

Thanks!

Thank you for helping to keep the Unisyn voting community secure!