SECURITY RESEARCH

# Vulnerability Notification and Control Program

*(May 3rd, 2023)*

Over the period of the last 15 years, Security Explorations has been notifying vendors of security vulnerabilities in their products, reported technical details of security issues found to vendors, provided vendors with access to all Proof-of-Concept codes and tools developed to illustrate the root cause of the issues, their impact or exploitation mechanism. This has been done completely unconditionally and for free. See Security Explorations in a Nutshell document for a summary of our activity.

While vendors didn't ask for our research to be delivered to them, taking into account the amount of time and dedication taken at our end and aimed at helping them make their products more secure, one would expect a smooth vulnerability handling process along the respect shown along the way.

As a result of experiencing significant disrespect / problems with various vendors, we decided to change our current approach and end what we have always perceived in terms of a courtesy to vendors.

**DISCLOSURE POLICY**

Security Explorations stops informing vendors about its security findings. By default, any such findings (results of Security Explorations' research) are to be disclosed to the public without prior notification (public and vendors learn about technical vulnerability details at the same time).

The new Disclosure Policy frees us from the burden of dealing with vendors over the vulnerability handling process (game plays regarding vulnerability confirmation, impact evaluation, fixing and disclosure, no responses to inquiries, etc.), yet it allows for a continuous contribution of our research results to the public. It lets us focus on our core R&D activity too, which is significant taking into account limited resources at our end.

We believe it is vendor's job and responsibility to perform quality vulnerability triage, fix the issues and communicate these to customers and the public. The new policy shouldn't limit

vendors in any way in that context, it simply moves all efforts / resources needed to complete vulnerability handling processes to the vendor's end (default scenario).

**SERVICES**

The following services are available for vendors willing to continue receiving private notification (vulnerability reporting), speed up its triage processes and/or assume some control over the disclosure process:

- *NOTIFICATION*
  notification 3 months prior to the publication of the results of our research at Security Explorations' web site about security issues potentially affecting given vendor's products and/or services. Notification is understood as a reporting of the technical details of the project without any Proof of Concept (PoC) Codes and tools

  Price: 24k EUR / year

- *CODES ACCESS*
  access to Proof of Concept (PoC) Codes and tools developed as part of a given project, NOTIFICATION subscription is required

  Price: project dependent

- *DISCLOSURE CONTROL*
  postponing of the disclosure (technical details publication at Security Explorations' web site) by 1 month (above the default 3 months), NOTIFICATION subscription is required, a maximum of additional 6 months can be claimed

  Price: 24k EUR / project

The above subscriptions give vendors a choice with respect to whether they prefer to receive security vulnerability information potentially affecting their products for free (from a public source) or in-private (on a fee basis). Vendors can also choose how detailed information they would like to receive (with or without codes access), if they would like to have an extra time for fixes development or would like to influence technical vulnerability details release to be delayed.