

OID Takeover due to IANA PEN Modification Request Incorrect Verification

This report concerns a vulnerability of ICANN's IANA's Private Enterprise Number (PEN) Registry website (<https://pen.iana.org/>) and how it incorrectly and exploitably handles requests to modify an Object Identifier (OID) assignment.

In particular, someone may request to modify the registration details for a PEN assignment at the website <https://www.iana.org/assignments/enterprise-numbers/assignment/modify/>. The modified information is filled-in and, for verification, an e-mail message is sent to the previous registration e-mail address contact person. If a modification of the contact e-mail address, then an e-mail message is also sent to the new e-mail address.

These two (2) e-mail messages request that the subject clicks on a supplied link to confirm the modifications.

The initial/current/previous e-mail address contact will be called "Owner" and the new e-mail address will be called "Requestor"

The vulnerability lies in the fact that the confirmation link sent to the Owner can be inferred from the confirmation link sent to the Requestor. Which means, that, conceivably, a Requestor can make a modification request, confirm it using his (Requestor's) confirmation link and then infer the Owner's confirmation link and use it to confirm the modifications on the Owner's behalf as well, in effect being able to unilaterally take over the -current- Owner's PEN OID.

One might think that the -current- Owner will have time to review the e-mail and take necessary corrective steps (e.g., contacting IANA) before the modifications take place, since IANA manually does the modifications, and it usually takes a few weeks. This, though, is not a countermeasure, and, moreover, many e-mail messages end up being classified as Spam and the -current- Owner might never have a chance to read the e-mail message that informs of his OID assignment's takeover.

Proof:

Below are the confirmation links sent when a modification is requested:

Owner:

<https://pen.iana.org/pen/app?page=ConfirmModificationDetail&service=external&sp=S?????&sp=Sowner>

Requestor:

<https://pen.iana.org/pen/app?page=ConfirmModificationDetail&service=external&sp=S?????&sp=Srequester>

The “?????” included in the links is representing a case/ticket number, which is unique for each modification request. From what can be seen, both confirmation links are otherwise identical, except the last part that says either “Sowner” or “Srequester”. Due to this pattern, one link can be inferred from the other.

To mitigate this, and also according to Best Practices, confirmation links must include a unique and random element, such thus each link can not be inferred from another (e.g., the links should also include a random string/code to verify the request).