Disorder in the Court

Description

Insufficient permission check vulnerabilities in public court record platforms from multiple vendors allowed unauthorized public access to sealed, confidential, unredacted, and/or otherwise restricted case documents. Affected documents include witness lists and testimony, mental health evaluations, child custody agreements, detailed allegations of abuse, corporate trade secrets, jury forms, and much more.

Details

Many of the platforms are developed by separate entities.

- **Catalis - CMS360** is used in Georgia, Mississippi, Ohio, and Tennessee. Catalis is a "government solutions" company that provides a wide array[1] of public record, payment, and regulatory/compliance platforms.
- **Henschen & Associates - CaseLook** is used in Ohio. Henschen & Associates did not respond after multiple reports, however the vulnerability has been fixed.
- **Tyler Technologies - Court Case Management Plus** is used in Georgia. In February, 2022 a different Tyler Technologies court records platform had a similar vulnerability that allowed the website judyrecords.com to accidentally scrape sensitive data.
- Five platforms used by individual courts in Florida -- **Brevard County**, **Hillsborough County**, **Lee County**, **Monroe County**, and **Sarasota County** -- are each presumed to be developed "in-house"[2] by the county court.
- *Note: Additional platforms from other vendors that are known to be vulnerable will be included in future disclosures.*

While all of the platforms allowed unintended public access to restricted documents, the severity varied due to the levels of restrictions that could be bypassed and the discoverability of document IDs. The methods used to exploit each of the vulnerabilities also varied, but could all be performed by an unauthenticated attacker using only a browser's developer tools.

Platforms

Catalis – CMS360

To view documents, URLs with numeric document and case IDs were used. This allowed an unskilled attacker to stumble upon restricted documents by simply incrementing the document ID in the document URL.

Many courts configured CMS360 to disallow document viewing altogether, making it very difficult to guess document IDs, so it is unclear whether documents could be viewed if document IDs were discovered. Many courts also require a login to view cases, so it is not known whether those courts allowed viewing images.

- CVE-2023-6341: Catalis (previously Icon Software) CMS 360 allows a remote, unauthenticated attacker to view sensitive court documents by modifying document and other identifiers in URLs. The impact varies based on the intention and configuration of a specific CMS360 installation.

Henschen & Associates – CaseLook

Document URLs were obfuscated using a bizarre format that interposed parts of the case number with a docket ID that started at zero and incremented for every document in the case, the length of the docket ID, the size of the file, and the length of the size of the file. The only information an attacker wouldn't know is the size of the file. A brute force was possible, however, the enumerable space grew with each page in the document.

The bigger problem was the way documents were served to the user. When a user requests a document URL, a copy of the file is placed into a cache directory before being served to the user. Files in the cache directory were stored with incrementing numeric filenames that ranged from 0 to 32,767 (for reference: the Super Nintendo, released in 1991, can count to 65,535). The counter incremented in an unknown way over time and was also incremented by 8 each time a new document was requested. If an attacker were to scan those filenames, they would have eventually discover documents, including those with restrictions.

Although Henschen & Associates eventually fixed the vulnerability, they did not ever respond to reports. This type of behavior is disrespectful to reporters of vulnerabilities and should give customers pause; if no response is received, future reporters may instead decide to sell, exploit, or immediately publish their discoveries.

- CVE-2023-6376: Henschen & Associates court document management software does not sufficiently randomize file names of cached documents, allowing a remote, unauthenticated attacker to access restricted documents.

Tyler Technologies – Court Case Management Plus

Multiple vulnerabilities were found in Court Case Management Plus.

The first vulnerability was a mechanism that enabled automatic passwordless login for any user, which was triggered by adding the query parameter `xyzldk=<username>` to the login URL; this was discovered through a simple Google search.

The second was a pair of vulnerabilities related to the use and misconfiguration of a very old, end-of-life component from Aquaforest called TIFF Server. The first of the pair allowed an attacker to enumerate the name of every file in a directory by adding the query parameter `PN=<number>` to `tssp.aspx`; if the file was a document, it could also be viewed. The second of the pair allowed an attacker to enumerate every directory on the system, and even more concerning, the entire network, by using `tiffserver.aspx` and either `te003.aspx` or `te004.aspx`. Combining this pair of vulnerabilities gave an attacker an extraordinary level of access to files far beyond those in a court case. In a number of instances, the enumeration led to the discovery of directly downloadable files, including as-yet-unfiled warrant applications and backups of source code for nine separate Tyler Technologies platforms.

In 2019, a similar vulnerability in TIFFServer (CVE-2020-9323) was discovered by Quentin (paragonsec) Rhoads-Herrera of TEAMARES that allowed an attacker to know how many files were in a directory. A second vulnerability (CVE-2020-9325) disclosed at the same time allowed an attacker to download arbitrary files. Court Case Management Plus was not affected by the latter vulnerability as the version being used was released an astonishing *14 years earlier*, in 2006. After being notified of the vulnerabilities, Aquaforest wrote a guide on how TIFF Server configurations can be made more secure.

- CVE-2023-6342: Tyler Technologies Court Case Management Plus allows a remote attacker to authenticate as any user by manipulating at least the 'CmWebSearchPfp/Login.aspx?xyzldk=' and 'payforprint_CM/Redirector.ashx?userid=' parameters. The vulnerable "pay for print" feature was removed on or around 2023-11-01.
- CVE-2023-6343: Tyler Technologies Court Case Management Plus allows a remote, unauthenticated attacker to enumerate and access sensitive files using the tiffserver/tssp.aspx 'FN' and 'PN' parameters. This behavior is related to the use of a deprecated version of Aquaforest TIFF Server, possibly 2.x. The vulnerable Aquaforest TIFF Server feature was removed on or around 2023-11-01.
- CVE-2023-6344: Tyler Technologies Court Case Management Plus allows a remote, unauthenticated attacker to enumerate directories using the tiffserver/te003.aspx or te004.aspx 'ifolder' parameter. This behavior is related to the use of a deprecated version of Aquaforest TIFF Server, possibly 2.x. The vulnerable Aquaforest TIFF Server feature was removed on or around 2023-11-01.
- CVE-2023-6353: Tyler Technologies Civil and Criminal Electronic Filing allows an unauthenticated, remote attacker to upload, delete, and view files by manipulating the Upload.aspx 'enky' parameter.
- CVE-2023-6354: Tyler Technologies Magistrate Court Case Management Plus allows an unauthenticated, remote attacker to upload, delete, and view files by manipulating the PDFViewer.aspx 'filename' parameter.
- CVE-2023-6375: Tyler Technologies Court Case Management Plus may store backups in a location that can be accessed by a remote, unauthenticated attacker. Backups may contain sensitive information such as database credentials.

- CVE-2023-6352: The default configuration of Aquaforest TIFF Server allows access to arbitrary file paths, subject to any restrictions imposed by Internet Information Services (IIS) or Microsoft Windows. Depending on how a web application uses and configures TIFF Server, a remote attacker may be able to enumerate files or directories, traverse directories, bypass authentication, or access restricted files.

Brevard County, Florida

Document URLs contain a version of the document ID that is encrypted using a method that includes an expiry mechanism. Although every docket entry displays the associated document ID, the encrypted form -- which is required to view documents -- is only provided for documents that the user has access to. This would be a great method that enables sharing of documents for a limited time, but for one fatal flaw.

Along with the encrypted document ID, the URLs also contain the query parameters `theIV=` and `theKey=`, which an astute observer might recognize as AES. Using the IV and key from the URL, an attacker can encrypt a document ID and use it to view a restricted document. Additionally, URLs include the parameter `isRedacted=` which, as the name suggests, accepts the encrypted form of the strings "Yes" or "No" to view unredacted copies of documents.

Hillsborough County, Florida

Session cookies are used to determine which cases and documents a user is viewing. When a case or document is requested, a request is sent to the API, which associates the data with the user's session cookie and returns the results. The API endpoint for obtaining document information returns a list that includes the document ID, several values that specify the security level required to view the document, and the user's applied access level. The frontend chooses whether to display a document link or one of the restriction type indicators based on the applied access level. The backend assumes that if an attacker is able to request a document, they must have access to it. An attacker can view restricted documents by changing the security level to a more permissive value.

Lee County, Florida

Session cookies are used to determine which cases and documents a user was viewing. When a case or document is requested, a request is sent to the API, which associates the data with the user's session cookie and returns the results. For most types of cases, document IDs are available in the pre-rendered HTML. Restricted documents could be viewed by executing the `pushDataAndShow()` function from the site's JavaScript source code.

Monroe County, Florida

A similar vulnerability was discovered initially, however their attempted fix introduced a new vulnerability. Much like Hillsborough County, the frontend chooses whether to display a document link based on the security level of the document and the backend incorrectly assumes that all requests should be trusted. After fixing the first vulnerability, the developers helpfully left a debugger statement immediately before the security level was checked, which paused code execution and gave an attacker a chance to adjust the security level and exploit this vulnerability. The debugger statement has since been removed and the backend no longer returns valid document IDs for restricted documents, however the backend still accepts restricted document IDs.

Sarasota County, Florida

In what is certainly the most egregious of the Florida county vulnerabilities, document URLs contained nothing more than a numeric document ID. An attacker could view restricted documents by simply incrementing the document ID in the URL. The only protection was a CAPTCHA on the landing page, which could be bypassed.

Given the ease with which this vulnerability could be discovered and exploited, it is reasonable to assume that every document was compromised the moment it was filed.

In defense of Sarasota County, they were the first to attempt to fix their issue. Unfortunately, their first attempt at a fix was not sufficient and a new vulnerability was discovered. Worse yet, while searching for a new method, a third vulnerability (or a second consequence of the second vulnerability) was discovered that allowed an unauthenticated attacker to view restricted cases.

Timeline

- 2023-06-21 - Vulnerability #1 discovered in Monroe County.
- 2023-07-04 - Report #1 sent to Monroe County – *no response*.
- 2023-07-14 - Report #2 sent to Monroe County – *no response*.
- 2023-07-17 - Vulnerability discovered in Catalis' CMS360.
- 2023-08-?? - **Vulnerability #1 confirmed fixed in Monroe County.**
- 2023-08-?? - Vulnerability #2 discovered in Monroe County.
- 2023-09-14 - Report for Monroe County and CMS360 vulnerabilities sent to Jason Parker at Jeltz by "Eli", for further research.
- 2023-09-15 - Vulnerability discovered in Lee County.
- 2023-09-15 - Vulnerability #1 discovered in Sarasota County.
- 2023-09-16 - Vulnerability discovered in Hillsborough County.
- 2023-09-18 - Vulnerability discovered in Brevard County.
- 2023-09-30 - Report #1 for CMS360 sent to Catalis – *no response*.
- 2023-10-02 - Report #2 for CMS360 sent to Catalis – *no response*.
- 2023-10-02 - Report for all vulnerabilities sent to CERT Coordination Center (CERT/CC).
- 2023-10-03 - Report for all Florida court vulnerabilities sent to Florida's Office of the State Courts Administrator (OSCA).
- 2023-10-03 - Report #3 for CMS360 sent to Catalis, detailing report to CERT/CC – *no response*.
- 2023-10-04 - Report for all vulnerabilities sent to Cybersecurity and Infrastructure Security Agency (CISA) by CERT/CC.
- 2023-10-06 - Report #4 for CMS360 sent to Catalis, with disclosure timeline and CISA hand-off details – *no response*.
- 2023-10-06 - Vulnerability #1 discovered in Tyler Technologies' Court Case Management Plus.
- 2023-10-06 - Response from Florida OSCA.
- 2023-10-06 - Report sent to Florida Court Clerks & Comptrollers by Florida OSCA.
- 2023-10-07 - Vulnerabilities #2 and #3 discovered in Court Case Management Plus.
- 2023-10-07 - Report for Court Case Management Plus sent to Tyler Technologies.
- 2023-10-08 - Response from Tyler Technologies.
- 2023-10-10 - Report for Court Case Management Plus sent to CISA.
- 2023-10-10 - Vulnerability discovered in Henschen & Associates' CaseLook.
- 2023-10-11 - Report #1 for CaseLook sent to Henschen & Associates – *no response*.
- 2023-10-11 - **Vulnerability #1 confirmed fixed by Sarasota County.**
- 2023-10-11 - Vulnerability #2 discovered in Sarasota County.
- 2023-10-13 - Report #2 for CaseLook sent to Henschen & Associates – *no response*.
- 2023-10-16 - Report #3 for CaseLook sent to Henschen & Associates – *no response*.
- 2023-10-17 - Report #4 for CaseLook sent to Henschen & Associates – *no response*.
- 2023-10-27 - **Vulnerability #2 confirmed fixed by Sarasota County.**
- 2023-11-01 - **Vulnerabilities #1, #2, and #3 in Court Case Management Plus confirmed fixed by Tyler Technologies.**
- 2023-11-01 - Response from Catalis, after discussion with CEO Scott Roza.
- 2023-11-03 - **Vulnerability in CMS360 confirmed fixed by Catalis.**
- 2023-11-13 - Report #5 for CaseLook sent to Henschen & Associates - *no response*.
- 2023-11-13 - Report for CaseLook sent to Ohio State CISO and Madison County, Ohio Court Clerk - *no response*.

- 2023-11-22 - **Vulnerability in CaseLook confirmed fixed by Henschen & Associates.**
- 2023-11-28 - **Vulnerability #2 confirmed partially fixed by Monroe County.**
- 2023-11-29 - **Vulnerability confirmed fixed by Lee County.**

Overview by Platform

Vendor	Platform	IDs Available	Access	Fix Date
Catalis / ICON Software	CMS360	No	R	2023-11-03
Tyler Technologies	Court Case Management Plus	Yes	RUZ	2023-11-01
Henschen & Associates	CaseLook	No	R	2023-11-22
Brevard County		Yes	RU	
Hillsborough County		Limited	R	
Lee County		Limited	RZ	2023-11-29
Monroe County		Yes	R	2023-11-28
Sarasota County		No	R	2023-10-27

Key:

- *IDs Available*:
  - Whether restricted document IDs are available to an attacker.
- *Access*:
  - *R* - Sealed, Confidential, Pending Redaction, and/or VOR (Viewable on Request).
  - *U* - Unredacted.
  - *Z* - Attackers can view partial details of cases marked as restricted.

Acknowledgements

- "Eli", who discovered the first set of court vulnerabilities and has been a major contributor throughout the process. *[Is this how most adults find and make friends?]*
- Andrew Crocker and Hannah Zhao from the Electronic Frontier Foundation, who were there in a time of need.
- Josh Renaud from St. Louis Post-Dispatch, who provided much needed early guidance and previously fought the fight that made it so I didn't have to, earning him a Press Freedom Award.
- Jaku founder of Crowd Control, who frequently offered his cybersecurity wisdom and experience.
- Zack Whittaker from TechCrunch, who immediately recognized the severity and jumped at the chance to learn more.
- judyrecords.com, who handled the first round of fallout from court security issues.
- The Arkansas Administrative Office of the Courts, who allowed me to present my findings in an effort to avoid the same pitfalls when building their own court platform.
- Dedications to the Fediverse furries, who provided plenty of amusement after my Bluesky / AT Protocol vulnerability publications. I see you.
- The CISA CVD Team assisted with the coordination of these vulnerabilities.

Contact

Jason Parker

- Email: north@⌒.com
- Press: press@jeltz.org
- Mastodon: @north@⌒.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. Several hundred hours of unpaid labor have been put into researching and disclosing these vulnerabilities; no vendors have provided or offered any bounties.

Definitions

- **Enumeration**: The process of systematically probing a system to discover valuable information, such as document names or user accounts, by incrementing values in a URL or input field.
- **Brute Force Attack**: A method of trial-and-error used to obtain information such as a password or PIN. In this case, it refers to repeatedly trying different document IDs to find restricted documents.
- **Obfuscation**: The practice of making something difficult, but not impossible, to understand. In a security context, obfuscation might be used to make files or code less readable, thereby hiding information from unauthorized users.
- **Developer Tools**: A set of tools included in most web browsers that allow developers to inspect the underlying code of a web page, monitor network requests, and test live JavaScript code among other functionalities.
- **Query Parameter**: A way to pass data in a URL, typically used in GET requests to web servers, which can be manipulated for purposes such as accessing unauthorized data.
- **Cache Directory**: A temporary storage location on a computer where frequently accessed data is kept to speed up retrieval.
- **AES**: A specification for the encryption of electronic data, standing for Advanced Encryption Standard.
- **Session Cookie**: A small piece of data sent from a website and stored by the user's web browser while the user is browsing, used to remember stateful information for the duration of the browsing session or some other expiry timeout.

Footnotes

1. *Catalis states on their website that "in less than five years [we have] strategically acquired and combined more than 30 public sector software companies". Learning and merging infrastructure after an acquisition takes a large amount of effort. Juggling 30 acquisitions would be a monumental undertaking that reduces focus on other necessary areas of business (e.g. securing legacy platforms).* ↩

2. *This is very uncommon in other states. A guess as to why Florida does things so differently is that Florida's extensive open records or "sunshine" laws (see also "Florida Man") spawned platforms before commercial vendors began to enter the market. Unlike many states where court records are made available through a single state website, Florida generally allows each county to make decisions about which platforms they use, as long as they follow Florida's Standards for Access to Electronic Court Records and Access Security Matrix.* ↩