Open Bug 2084460 Opened 17 days ago Updated 5 hours ago

DigiCert: Unauthorized access to business system

Categories

Product: CA Program
Component: CA Certificate Compliance
Type: task
Priority: *Not set* Severity: --

Tracking

Status: ASSIGNED

People (Reporter: dcbugzillaresponse, Assigned: dcbugzillaresponse)

Details (Whiteboard: [ca-compliance] [policy-failure])

Bottom ↓ Tags Timeline

DigiCert Assignee
Description • 17 days ago

Preliminary Incident Report

Summary

- **Incident description:** DigiCert has identified an event involving unauthorized access to one of our business systems that stores information customer representatives provide to us to validate their identity. No certificate operations were impacted.
- **Relevant policies:** Mozilla Policy 2.4.1
- **Source of incident disclosure:** Self Reported

incident-reporting
Updated • 16 days ago

Assignee: nobody → dcbugzillaresponse
Status: UNCONFIRMED → ASSIGNED
Ever confirmed: true
Whiteboard: [ca-compliance] [policy-failure]

DigiCert Assignee
Comment 1 • 10 days ago

DigiCert will provide our full incident report on or before 2026-11-03.

Full Incident Report

Note: This is a disclosure of a security incident affecting a business system used to archive business contact and personal information provided by customers. This incident affected only a small proportion of archived data.

DigiCert's Certificate Authority (CA) services, CertCentral, and DigiCert ONE were unaffected and remain secure. Customer login credentials and DigiCert-issued certificates remain secure, valid, and fully trusted. No action is needed from customers regarding active certificates and continued use of DigiCert services.

Summary

- **CA Owner CCADB unique ID:** A000021
- **Incident description:** DigiCert identified an event involving unauthorized access to an internal business system which is used to archive information provided by customers. Such information included the business contact information and, in some cases, additional personal information of customer representatives.

  On 2025-02-04, the internal business system was moved from a VPN-restricted network segment to a different availability zone. This migration inadvertently allowed this internal business system to be accessible externally. The business system uses an account manager system. A feature for account registration intended for other use cases was part of the account manager, and inadvertently became available to this business system.

  As the business system was not intended to use this account creation feature, accounts registered through this endpoint were not subject to the multi-factor authentication (MFA) that DigiCert otherwise requires, and were assigned read-only mode by default. However, these unassigned accounts had access to archived data on the business system.

  DigiCert maintains policies and processes to identify and remediate security vulnerabilities, including those arising from our participation in a managed security research program. Beginning on 2026-06-21, DigiCert determined that the business system was externally accessible when that was not intended, and that an unassigned account had been created. DigiCert deployed an authorization fix on 2026-07-02 that remediated account creation and disallowed access to archived data by unassigned accounts. At this time DigiCert was unaware that a small proportion of archived data had been accessed by the account created.

  On 2026-10-19, DigiCert confirmed unauthorized access to a subset of archived data and determined this to be a reportable event. Most of the data was limited to business contact information for customers: names, business email addresses, phone numbers, and business addresses. A small minority of customer accounts included additional personal data in the form of a customer-provided

document such as a driver's license, passport, utility bill, or other document with name and address. The access could not write records, act as a validation approver, or issue certificates.

- **Timeline summary:**
  - **Non-compliance start date:** 2025-02-04 business system is externally accessible, (access to data occurred later ~ 2026-06-27).
  - **Non-compliance identified date:** 2026-06-21.
  - **Non-compliance end date:** 2026-07-02 account registration end-point access terminated.
- **Relevant policies:**
  - Mozilla Root Store Policy, Section 2.4.
  - Chrome Root Program Policy, Section 1.5.1.
  - Microsoft Trusted Root Program Policy, Section 2.1.18.
  - Apple Root Certificate Program, Section 3.
- **Source of incident disclosure:** Self Reported

Impact

- **Total number of certificates:** 0. No certificates were affected by this incident.
- **Total number of "remaining valid" certificates:** N/A
- **Affected certificate types:** N/A. No certificates were issued, modified, or revoked as a result of this incident.
- **Incident heuristic:** N/A. This incident involved read-only access to information held in an internal business system and did not affect validation outcomes, certificate issuance, or certificate content.
- **Was issuance stopped in response to this incident, and why or why not?:** No. Access was limited to read-only access to archival information and did not provide an ability to perform or approve validations or request, approve, or issue certificates. The CA systems operate on their own secure network segments and were not affected by this external access. For confirmation, logs review of CA and validation activity found no validation actions, certificate issuance, or revocation activity associated with the associated account.
- **Analysis:** N/A.
- **Additional considerations:** N/A.

Timeline

Date	Event
2025-02-04	As part of an infrastructure migration, the business system is moved from a VPN-restricted segment to an availability zone that was externally accessible.
2026-06-18	DigiCert internal team observes non-DigiCert accounts on the business system. As the accounts were not assigned to any application, the reviewer concludes they did not have data access. The business system is moved behind Web Application Firewall (WAF), blocking new account creation through external access.
2026-06-21	DigiCert receives report from managed security program indicating possibility for account creation through external access.
2026-06-24	DigiCert verifies the account creation ability.
2026-06-27	Start of the data access window (shown by subsequent investigation).
2026-06-30	Root cause for external account creation is identified by Engineering.
2026-07-01	Software patch for external account creation is created and tested/ready for production.
2026-07-02	Software patch with an authorization restriction is released to production for the business system. End of the data access window (confirmed by subsequent investigation).
2026-07-09	The WAF restricts the business system hostnames to VPN traffic only, except for approved externally-accessible endpoints.
2026-08-28	Policy requiring security sign-off for network access control changes on internal tools is updated.
2026-08-31	Penetration test of the business system and related internal tools is completed by external vendor.
2026-10-12	DigiCert first suspects possible unauthorized access to the archived data, begins additional investigation.
2026-10-15	DigiCert institutes additional monitoring and alerting on file access and request volumes. All remaining non-DigiCert accounts, used for pen test, are verified as removed.
2026-10-17	Password resets are completed for all the business system users. The internal endpoints involved are validated as returning 401 to unauthorized access.
[illegible]	Determination of reportable event under Browser root policy program requirements.

2026-10-19	Investigation determines the data access window as 2026-06-27 through 2026-07-02 with corroboration on file access and request volumes.
2026-10-20	Preliminary Incident Report filed for this event.
2026-10-24	The feature that permitted self-registered users is deactivated for all business system instances. Remaining externally accessible business system endpoints are moved onto private-IP load balancers and internal hostnames. Scan shows no externally accessible business system endpoint.
2026-10-29	Ownership for the business system's security posture is clarified, with responsibility for confirming WAF, monitoring, and access review coverage whenever accessibility changes.
2026-10-30	Least-privilege review of the permissions model is completed. Each subsystem endpoint confirmed to enforce authorization by checking application assignment and role.

Related Incidents

The following recent related incidents dealt with privacy and management of archive data.

Bug	Date	Description
2086949	2026-10-29	TWCA: Unauthorized access to an RA server.
2085547	2026-10-24	D-Trust: Loss of archived RA records for S/MIME certificates at E.ON SE RA

Root Cause Analysis

Root Cause Analysis methodology used: Five Whys, conducted with security engineering, the business system engineering, platform engineering, security operations, industry standards, and compliance.

Technical background: The business system utilizes an account manager that DigiCert also uses for customer-facing products. The business system runs its own instances of that platform, separate from the customer-facing instance. DigiCert staff are "system users" on that instance and sign in through MFA. An account manager optional feature provides a self-service registration flow for customer sign-up on other implementations. That flow does not use MFA and was inadvertently provided to the business system.

Contributing Factor #1: the business system's network accessibility changed without a security review of the resulting attack surface

- **Description:** During the February 2025 infrastructure migration, the business system, an internal system never intended to be externally accessible, was moved from a VPN-restricted segment to an availability zone. This inadvertently made the account registration endpoint externally accessible. Additionally, MFA is only enabled if the account is assigned to an application that requires MFA.

- **Timeline:** Migration on 2025-02-04. Closed on 2026-07-02.
- **Detection:** It was not detected earlier because the migration was treated as an infrastructure change rather than a security change which would have triggered more detailed review and sign off.
- **Interaction with other factors:** This factor created the entry point. It persisted undetected because of CF #2.

Contributing Factor #2: Insufficient monitoring and alerting on business system account activity

- **Description:** The business system was intended for internal access via the VPN and MFA. Monitoring requirements had not been reassessed after the migration. The business system had insufficient alerting for new account creation through the externally-accessible endpoint or request volume from its internal endpoints.
- **Timeline:** The monitoring gap became material on 2025-02-04 when the network accessibility changed. A Security Information and Event Management (SIEM) alert on blocked access to the business system was in place by 2026-07-02. Additional application-level access alerts and a request-volume alert were added on 2026-10-15.
- **Detection:** The gap was confirmed during the investigation.
- **Interaction with other factors:** When the business system inadvertently became externally accessible via CF #1, there was insufficient ability to alert upon the unauthorized access.

Contributing Factor #3: The business system authorization model did not contemplate self-registration

- **Description:** The business system authorization implemented MFA requirements to access the system. Following the migration (CF #1), a self-registered account with no application assigned could have read-only access to data.
- **Timeline:** The read-only access to data first occurred on 2026-06-27. An authorization change to validate the token issued by the account manager and return HTTP 401 to any account with no assigned application, was released to production on 2026-07-02.
- **Detection:** It was not detected earlier because initial reviews concluded incorrectly, from the absence of an assigned application, that the account had no data access.
- **Interaction with other factors:** Made CF #1 actionable to read-only access.

Lessons Learned

- **What went well:**
  - The authorization fix released in July prevented future attempts to access the data.
  - Detailed logs and audit tables were retained, which allowed the access list, the access window, and the account-to-activity attribution to be reconstructed. The log and audit data also allowed us to confirm that the CA was not accessed and that no validation records were changed by the account.
  - Our investigation confirms the account performed no write actions.
- **What didn't go well:**

    - The incident was initially handled as an account-creation issue rather than a data-access event.
- **Where we got lucky:** N/A.
- **Additional:**
    - Network accessibility changes to internal systems should always require a security review.
    - Authorization for a business system must not be delegated to its network position.

Action Items

#	Action Item	Kind	Corresponding Root Cause(s)	Evaluation Criteria	Due Date	Status
1	Block the account registration endpoint at the WAF for the business system hostnames	Mitigate	CF #1	No account creation through the WAF-fronted path after 2026-06-18, confirmed in WAF logs	2026-06-18	Complete
2	Release change so that internal endpoints return 401 for any account with no assigned application. Disallowed access to archived data by unassigned accounts.	Prevent	CF #3	Verified in QA and production; forensic validation on 2026-10-17	2026-07-02	Complete
3	Restrict the business system hostnames at the WAF to VPN traffic only, with an explicit list of approved externally-accessible endpoints	Mitigate	CF #1	Updated WAF policy in place	2026-07-09	Complete
	Updates to policy requiring security sign-			Policy published internally; change		

4	off and an asset inventory update for any change to the network accessibility of internal tools	Prevent	CF #1, CF #2	[illegible] management records for subsequent network accessibility changes show security approval	2026-08-28	Complete
5	Conduct a penetration test of the business system and related internal tools after the authorization and network changes	Prevent	CF #1, CF #2	Test completed; findings remediated	2026-08-31	Complete
6	Add application-level alerts on file access and request volumes, independent of the WAF, and an alert, routed to SOC	Detect	CF #2	Alerts enabled; the 2026-07-01 request volume would have triggered the alert	2026-10-15	Complete
7	Password resets are completed for all the business system users.	Mitigate	CF #1	Business system is validated as returning 401 to unauthorized access	2026-10-17	Complete
	Deactivate the self-registration			No account on the		

8	feature on business system instances.	Prevent	CF #1		business system instance outside MFA	2026-10-24	Complete
9	Remaining externally accessible endpoints transitioned to private-IP load balancers and internal hostnames	Prevent	CF #1		External scan shows no externally-accessible business system endpoint	2026-10-24	Complete
10	Assign a single named owner for the business system's security posture, responsible for confirming WAF, monitoring, and access review coverage whenever accessibility changes	Prevent	CF #1		Owner named in the asset inventory; sign-off recorded for each subsequent accessibility change	2026-10-29	Complete
11	Complete the least-privilege review of the subsystem permissions model and enforce authorization	Prevent	CF #3		Each business system endpoint checks application assignment and role	2026-10-30	Complete

	per endpoint						
12	Confirm by internal audit that no business system origin server is externally accessible	Prevent	CF #1		External attack surface scan shows no externally accessible origin	2026-11-06	Ongoing
13	Final review of existing automated alerting for unexpected account creation and changes to account or user permissions for the business system, including accounts created outside approved provisioning workflows, routed to Security Operations with a defined escalation path	Detect	CF #1, CF #2		Alerts live; investigation and escalation procedure documented	2026-11-06	Ongoing

Appendix

No certificates were affected by this incident, so no certificate listing is attached.