



Executive Summary

CISA published two medical advisories on September 10, and the first is the most consequential medical device advisory this series has covered. ICSMA-26-253-01 discloses three vulnerabilities in NextGen Healthcare Mirth Connect versions 4.7.1 and earlier — CVE-2026-82583, CVE-2026-78224 and CVE-2026-82578 — comprising SQL injection and XML external entity weaknesses. Mirth Connect is the HL7 integration engine that sits between electronic health records, laboratory and radiology systems, PACS, and billing platforms across a very large share of US hospitals, health systems, laboratories and health information exchanges. The reason this matters more than its CVSS scores suggest is in the CVE record for CVE-2026-82583: an authenticated user executing arbitrary SQL through a Database Connector API could obtain disclosure of stored credentials for connected systems, along with arbitrary file write and denial of service. An integration engine holds credentials for everything it integrates with. Compromising it is not one system lost; it is the keys to the clinical data pipeline. One of the three flaws, CVE-2026-82578, requires no privileges at all. NextGen has released v4.7.2, and the correct response is to patch and then rotate every downstream credential the engine holds.

The second advisory, ICSMA-26-253-02, covers CVE-2026-87020 in Orthanc DICOM Server versions earlier than 1.13.0, where an integer overflow allows an authenticated remote attacker to write past the end of a heap allocation when Orthanc decodes a crafted PNG or JPEG image, crashing the process. CVSS v3 8.1, with no known public exploitation. Orthanc is the fifth distinct DICOM product line to draw a CISA advisory in the current run, after GDCM, pydicom/pynetdicom, DCMTK and RadiAnt — and it extends the pattern from libraries and viewers to the server tier.

On the intelligence side, for the second consecutive week a GTI operation record confirms a US healthcare organisation as a victim. OP.26.1312, created September 11, documents UNC7072 targeting a healthcare subsector organisation in August 2026 using the CLOUDHAZE malware family, with command-and-control established through domains including apexesmasters.com and familypenguins.com. Also this week, CAMP.26.131 documents the NATIVEPIPE backdoor persisting through legitimate RMM tools, malicious browser extensions, Python runtimes and QEMU virtual machines used for SSH port forwarding. On breaches, Boston Scientific disclosed in an SEC filing on September 8 that the August cyberattack means it is unlikely to meet sales growth and adjusted earnings guidance for either the third quarter or the full year — the first quantified financial consequence of a medtech supply disruption this series has tracked — and Veradigm disclosed a patient data breach originating at a third-party vendor.

Active Threat Campaigns- Healthcare & Technology

Advisory / Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
NextGen Healthcare Mirth Connect — SQL Injection and XXE (CISA ICSMA-26-253-01, Sep 10)	Medical software vulnerability — clinical integration engine	Three vulnerabilities in NextGen Healthcare Mirth Connect (formerly NextGen Connect) versions 4.7.1 and earlier: CVE-2026-82583, CVE-2026-78224 and CVE-2026-82578. The weaknesses are SQL injection (CWE-89) and improper restriction of XML external entity references (CWE-611). CISA states successful exploitation could allow an attacker to exfiltrate data or cause a denial-of-service condition. The CVE record for CVE-2026-82583 is more specific and more serious: an authenticated user can execute arbitrary SQL through a Database Connector API, which could result in DISCLOSURE OF STORED CREDENTIALS FOR CONNECTED SYSTEMS, arbitrary file write, and denial of service. CVE-2026-82583 is CVSS v3.1 8.3 and requires low privileges; CVE-2026-82578 is CVSS v3.1 7.5 / v4.0 8.7 and requires NO	Healthcare and Public Health — deployed worldwide, heavily concentrated in US hospitals, health systems, laboratories and health information exchanges. Mirth Connect is the HL7 integration engine sitting between EHR, LIS, RIS, PACS and billing systems	CRITICAL — Update to Mirth Connect v4.7.2 or later from the NextGen customer portal. Because stored credentials for CONNECTED systems may be disclosed, rotate every downstream integration credential held in Mirth after patching



Advisory / Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
		privileges. Reported to CISA by Abhinav Agarwal		
Orthanc DICOM Server — Heap Write via Crafted Image (CISA ICSMA-26-253-02, Sep 10)	Medical imaging software vulnerability	CVE-2026-87020 in Orthanc DICOM Server versions earlier than 1.13.0. An integer overflow or wraparound (CWE-190) allows an authenticated remote attacker to write past the end of a heap allocation when Orthanc decodes an attacker-supplied PNG or JPEG image, resulting in a crash of the Orthanc process and a denial-of-service condition. CVSS v3 8.1. CISA reports no known public exploitation and the CVE is not listed in the KEV catalog. Orthanc is a widely used open-source DICOM server and PACS component, frequently embedded in research imaging pipelines, teaching hospitals and smaller imaging estates	Healthcare and Public Health. This is the FIFTH distinct DICOM product line to draw a CISA advisory in the current run, after GDCM, pydicom/pynetdicom, DCMTK and RadiAnt	HIGH — Upgrade Orthanc to 1.13.0 or later. Authentication is required, so prioritise instances where DICOM credentials are shared, default, or widely distributed across research and clinical users
UNC7072 CLOUDHAZE Command and Control in Healthcare (OP.26.1312)	Targeted intrusion operation (motivation unknown)	A single-victim operation record. GTI reports that UNC7072 targeted a healthcare subsector organisation in August 2026 using the CLOUDHAZE malware family to facilitate unauthorised access. The operation leveraged several malicious domains, including apexesmasters.com and familypenguins.com, to establish command-and-control infrastructure. GTI assesses the activity demonstrated intent to maintain a persistent foothold within the single targeted environment for downstream mission objectives. Activity observed August 7–8, 2026; 29 mapped ATT&CK techniques	Healthcare GTI-confirmed — United States. This is the second consecutive week in which a GTI operation record confirms a US healthcare organisation as a victim, following UNC7032 SPINCHAIN in the September 4 brief	HIGH — Block and retro-hunt apexesmasters.com and familypenguins.com across DNS, proxy and firewall logs. Treat any resolution as an incident given the confirmed healthcare victimology
NATIVEPIPE Backdoor via Browser Extensions, RMM and QEMU Tunnelling (CAMP.26.131)	Persistent access and data collection (motivation unknown; actor UNC7083)	Deployment of the NATIVEPIPE backdoor, with persistence and command-and-control maintained through legitimate RMM tools, scheduled tasks, and QEMU virtual machines used for SSH port forwarding — a notable evasion: tunnelling traffic through a virtual machine places the network path outside the visibility of host-based monitoring on the physical endpoint. Malicious browser extensions and Python runtimes are used for persistent access. Automated reconnaissance and credential harvesting identify and stage sensitive corporate data for exfiltration to external file-sharing platforms. GTI maps 103 ATT&CK techniques, among the broadest footprints recorded in this series	GTI-confirmed: Legal & Professional Services, Manufacturing, Technology — United States. Healthcare NOT confirmed. Carried because legitimate-RMM persistence is the pattern the federal Medusa advisory documented against healthcare, and browser extensions are an unmanaged software layer in most clinical environments	HIGH — Alert on QEMU or other hypervisor binaries on endpoints where virtualisation is not sanctioned, on unexpected Python runtimes, and on browser extension installation outside managed policy. Inventory and allowlist RMM tooling

Top 4 Priority Actions This Week

1. [CRITICAL] Patch Mirth Connect and Rotate Every Downstream Credential It Holds

CISA published ICSMA-26-253-01 on September 10, 2026, disclosing three vulnerabilities in NextGen Healthcare Mirth Connect affecting all versions 4.7.1 and earlier. The underlying weaknesses are improper neutralisation of special elements used in an SQL command (SQL injection, CWE-89) and improper restriction of XML external entity reference (XXE, CWE-611). CISA's summary states that successful exploitation could allow an attacker to exfiltrate data or cause a denial-of-service



condition. The published CVE record for CVE-2026-82583 is more specific: NextGen Connect (Mirth Connect) versions 4.7.1 and earlier allow an authenticated user to execute arbitrary SQL through a Database Connector API, which could result in disclosure of stored credentials for connected systems, arbitrary file write, and a denial-of-service condition. CVE-2026-82583 carries CVSS v3.1 8.3 and requires low privileges; CVE-2026-82578 carries CVSS v3.1 7.5 and CVSS v4.0 8.7 and requires no privileges. The product is deployed worldwide with heavy concentration in United States hospitals, health systems, laboratories and health information exchanges. NextGen recommends updating to Mirth Connect v4.7.2 or later, available from the NextGen Healthcare customer portal. CISA has not reported confirmed in-the-wild exploitation and these CVEs are not listed in the KEV catalog. The vulnerability was reported to CISA by Abhinav Agarwal.

The architectural point deserves emphasis when briefing clinical and executive leadership. An integration engine exists precisely to hold connections — and therefore credentials — for every system it routes between: the EHR, laboratory and radiology information systems, PACS, pharmacy, scheduling and billing. A vulnerability that discloses stored credentials for connected systems converts a single application compromise into credentialed access across the clinical data estate. Patching closes the vulnerability; it does not invalidate credentials that may already have been read.

- Update Mirth Connect to v4.7.2 or later as the immediate action, including any instances operated by vendors, managed service providers, or inherited through acquisition
- After patching, rotate every credential stored in Mirth channel and connector configurations — database accounts, API keys, SFTP credentials, and service accounts for every connected downstream system. This is the step most organizations will skip and it is the one that matters
- Restrict network access to the Mirth Administrator interface and the Database Connector API to a management network; neither should be reachable from general clinical VLANs, let alone the internet
- Review Mirth database and application logs for anomalous SQL through the Database Connector API, and for unexpected file writes by the Mirth service account
- Alert on the Mirth Connect Java process spawning cmd.exe, PowerShell or a shell interpreter — an integration engine has no legitimate reason to launch a command shell, making this a high-fidelity post-exploitation signal
- Ask your EHR and integration vendors in writing whether Mirth Connect is embedded in any product they supply you; it is frequently bundled rather than separately procured

2. [HIGH] Upgrade Orthanc and Consolidate the Five-Product DICOM Position

ICSMA-26-253-02, published the same day, covers CVE-2026-87020 in Orthanc DICOM Server versions earlier than 1.13.0. The flaw is an integer overflow or wraparound allowing an authenticated remote attacker to write past the end of a heap allocation when Orthanc decodes an attacker-supplied PNG or JPEG image, resulting in a crash of the Orthanc process and a denial-of-service condition. CVSS v3 is 8.1, authentication is required, and CISA reports no known public exploitation. Orthanc is a widely deployed open-source DICOM server used as a PACS component, a research imaging archive, and a routing node in teaching hospitals and smaller imaging estates, and it is frequently stood up by clinical or research teams outside the managed software catalogue. With this advisory, five distinct DICOM product lines now carry CISA advisories in the current run: GDCM and pydicom/pynetdicom with no vendor fix and unresponsive maintainers, and DCMTK, RadiAnt and now Orthanc with fixes available. The useful framing for leadership is that the DICOM ingestion and processing chain — not any single product — is under sustained research attention, and the same compensating controls cover all five.

- Upgrade Orthanc to 1.13.0 or later across clinical, research and teaching deployments, and specifically look for instances stood up outside IT procurement
- Because exploitation requires authentication, prioritise instances where DICOM credentials are shared, default, or distributed across a wide research user base — that is where the authentication requirement provides least protection



- Apply the standing DICOM control set, which now covers all five affected product lines: block DICOM ingestion from unauthenticated sources, segment imaging networks, validate files at the boundary, and open imaging files only from trusted sources
- Complete the patchable items — DCMTK, RadiAnt and Orthanc — and document the compensating controls for GDCM and pynetdicom in your risk analysis records, since those two will not be fixed

3. [HIGH] Hunt UNC7072 CLOUDHAZE Infrastructure — Confirmed US Healthcare Victim

GTI created operation record OP.26.1312 on September 11, documenting that the threat actor UNC7072 targeted a healthcare subsector organization in August 2026, using the CLOUDHAZE malware family to facilitate unauthorized access. The operation leveraged several malicious domains, including apexesmasters.com and familypenguins.com, to establish command-and-control infrastructure. GTI assesses that the activity demonstrated the actor's intent to maintain a persistent foothold within the single targeted environment for downstream mission objectives, with activity observed on August 7 and 8 and 29 mapped ATT&CK techniques. This is the second consecutive week in which a GTI operation record has confirmed a US healthcare organization as a victim, following the UNC7032 SPINCHAIN operation reported in the September 4 brief.

- Block and retro-hunt apexesmasters.com and familypenguins.com across DNS, proxy and firewall logs for at least 90 days; treat any resolution as an incident given the confirmed healthcare victimology
- Given the malvertising delivery route documented in the linked campaign, review web filtering coverage for advertising networks and invoice or billing-themed sites, which are routinely visited by finance and revenue-cycle staff
- Alert on scheduled task creation followed by reconnaissance of running processes, installed security software, and browser profile data — the documented CLOUDHAZE post-execution sequence
- Brief revenue cycle, accounts payable and procurement teams specifically; invoice-themed lures target those roles, and they frequently hold access to financial and patient billing systems

4. [HIGH] Detect Virtualisation and Browser Extensions Used as Persistence (CAMP.26.131)

GTI released CAMP.26.131 on September 11, documenting deployment of the NATIVEPIPE backdoor with persistence and command-and-control maintained through legitimate RMM tools, scheduled tasks, and QEMU virtual machines used for SSH port forwarding, alongside malicious browser extensions and Python runtimes for persistent access. Automated reconnaissance and credential harvesting are used to identify and stage sensitive corporate data for exfiltration to external file-sharing platforms. GTI maps 103 ATT&CK techniques to this campaign, among the broadest footprints recorded in this series, and attributes it to UNC7083 with confirmed targeting of Legal & Professional Services, Manufacturing and Technology in the United States. Healthcare is not confirmed. Two techniques make it worth carrying anyway. Running a QEMU virtual machine to tunnel SSH traffic places the network path inside a guest that host-based monitoring on the physical endpoint cannot see — an evasion that defeats EDR visibility without disabling EDR. And malicious browser extensions are an almost entirely unmanaged software layer in most clinical environments, where clinicians install productivity and reference tools on shared workstations without review.

- Alert on QEMU, VirtualBox or other hypervisor binaries executing on endpoints where virtualization is not a sanctioned workload — this is rare enough in clinical and administrative estates to be high-fidelity
- Alert on unexpected Python runtime installation or execution on endpoints outside development and research populations



- Bring browser extensions under management: enforce an allowlist through Chrome or Edge policy, and inventory what is currently installed across clinical workstations, which for most organizations will be the first time that question has been answered
- Inventory and allowlist RMM tooling, then alert on any remote access agent outside the approved set — the same control the updated federal Medusa advisory called for against healthcare
- Monitor for bulk uploads to external file-sharing platforms from clinical and administrative endpoints

Healthcare Sector Incident Watch

Boston Scientific: The Financial Consequence Quantified

Boston Scientific disclosed in an SEC filing published Tuesday, September 8 that the cyberattack reported in the August 28 brief caused sufficient disruption that the company is unlikely to meet its sales growth and adjusted earnings guidance for either the third quarter or the full year 2026. The company said it does not expect the incident to materially affect its long-term financial condition. This is the first time in this series that a healthcare cyberattack has produced a quantified, publicly disclosed financial consequence at this scale, and it is worth using in internal risk conversations: the August intrusion knocked order-processing and shipping systems offline for the supply of pacemakers, defibrillators, stents and other implantable devices, and the recovery has been long enough to move full-year guidance for a major medtech manufacturer. For healthcare provider organisations the practical implication is unchanged from the August 28 brief — continue to manage implantable device supply actively rather than assuming normal lead times — but the disclosure confirms that the disruption has been material and extended rather than short-lived.

Veradigm and the Continuing Third-Party Pattern

Healthcare technology company Veradigm disclosed a data breach after a cybersecurity incident at one of its third-party vendors exposed patients' personal data, with a ransomware group claiming the attack. Separately, two ransomware groups have claimed attacks on the nationwide home healthcare provider Interim Healthcare. The Veradigm disclosure follows the same shape as the SickKids and McKesson incidents reported in the August 28 and September 4 briefs: the compromise occurred at the vendor's vendor, not at the healthcare organization and not at its direct supplier. Fourth-party risk is now the most consistent single theme across healthcare breach disclosures in this series, and it is the layer least covered by standard Business Associate Agreement due diligence.

- Ask your major vendors to disclose their own critical sub processors for any service that touches PHI, and record the answers — most BAA reviews stop at the direct relationship
- Where a vendor cannot or will not identify its sub processors, treat that as a finding and weight it in vendor risk scoring rather than accepting it as normal commercial practice
- For Veradigm and Interim Healthcare, if either is in your supply chain, request written status on whether your patient population is in scope and diary follow-up

Medical Device and IoT Security

Both new advisories are covered in Priority Actions 1 and 2. The tracker position after this week: ICSMA-26-253-01 (Mirth Connect $\leq$ 4.7.1, three CVEs, fix in v4.7.2) and ICSMA-26-253-02 (Orthanc $<$ 1.13.0, CVE-2026-87020, fix in 1.13.0) are both patchable and should be closed quickly. The three at-home Bluetooth device advisories remain open, with Pulsetto still carrying no vendor fix and an unresponsive vendor. Five DICOM product lines now carry advisories, of which GDCM (week 25, no patch) and pydicom/pynetdicom (no fix, maintainer unresponsive to CISA) remain permanent compensating-control problems while DCMTK, RadiAnt and Orthanc are patchable.



A structural observation for planning purposes. Across the last six weeks the medical device advisories have moved steadily inward: from patient-worn and at-home devices (Flow Neuroscience, Pulsetto, Mira), through clinical viewers and imaging libraries (RadiAnt, DCMTK, GDCM, pynetdicom), to laboratory instrumentation (Thermo Fisher Applied Biosystems), and now to the imaging server and the HL7 integration engine that connect the clinical estate together. The Mirth Connect advisory in particular sits at the point where medical device security and enterprise IT security stop being separable, because the same engine routes device output, clinical results and billing data. Organizations that have kept biomedical and IT security governance separate should treat this week as the argument for a joint review.

Persistent CVE and Advisory Tracker

CVE / Advisory	System / Component	CVSS	Advisory	Patch	Status & Action
CVE-2026-82583 / CVE-2026-78224 / CVE-2026-82578 (NEW)	NextGen Healthcare Mirth Connect ≤ v4.7.1	8.3 / 7.5 (v3.1); 8.7 (v4.0 for -82578)	CISA ICSMA-26-253-01 (Sep 10)	Yes	SQL injection (CWE-89) and XXE (CWE-611). CVE-2026-82583 allows an authenticated user to execute arbitrary SQL via a Database Connector API, enabling disclosure of stored credentials for connected systems, arbitrary file write and DoS. CVE-2026-82578 requires no privileges. Update to v4.7.2+, then rotate all downstream integration credentials. No confirmed in-the-wild exploitation; not in KEV.
CVE-2026-87020 (NEW)	Orthanc DICOM Server < 1.13.0	8.1 (v3)	CISA ICSMA-26-253-02 (Sep 10)	Yes	Integer overflow or wraparound (CWE-190); an authenticated remote attacker can write past the end of a heap allocation when Orthanc decodes a crafted PNG or JPEG, crashing the process. Upgrade to 1.13.0+. No known public exploitation.
CVE-2026-18844	Pulsetto Vagus Nerve Stimulator — ALL versions	Not published	CISA ICSMA-26-223-02	NO	Undisclosed BLE commands accepted without authentication permit disabling of electrical safety mechanisms. Vendor unresponsive to CISA; no fix. Patient counselling is the only control.
8 CVEs (CVE-2026-66875 et al.) / ICSMA-26-225-01	Mira Hormone Monitor and Android App; Flow Neuroscience FL-100 tDCS headsets	Not published	ICSMA-26-223-01 / -225-01	See advisory / Yes	Mira: unauthenticated BLE rebinding, cleartext hormone data extraction, user tracking via non-rotating BLE address. FL-100: hard-coded credential shared across all units permitting stimulation parameter manipulation — confirm firmware update via the Flow app.
CVE-2026-17583 / CVE-2026-17264	Thermo Fisher Applied Biosystems HID software; Medixant RadiAnt DICOM ≤ 2025.2	8.2 / 5.3 (v4.0)	ICSMA-26-216-01 / -218-01	Yes	Instrument output file tampering and heap out-of-bounds write via crafted DICOM pixel data. Update RadiAnt to 2026.1; three end-of-life Applied Biosystems products receive no update.



CVE / Advisory	System / Component	CVSS	Advisory	Patch	Status & Action
CVE-2026-50003 (+4 high)	OFFIS DCMTK Toolkit ≤ 3.7.0	9.8	CISA ICSMA-26-181-01	Yes	Path traversal via bit-preserving C-GET plus four high-severity flaws. Deploy the patched release; press imaging vendors on embedded copies.
CVE-2026-56445 / CVE-2026-3650	pydicom / pynetdicom qrscp; Grassroots DICOM (GDCM) 3.2.2	9.1 / 7.5	ICSMA-26-176-01 / -083-01	NO / NO	Both maintainers remain unresponsive to CISA. GDCM reaches week 25 without a patch. Maintain the shared DICOM control set across all five affected product lines.
CVE-2026-0257 / CVE-2025-53770	Palo Alto GlobalProtect VPN; Microsoft SharePoint	9.1 / see vendor	CISA KEV; GTI CAMP.26.077	Yes	GlobalProtect KEV deadline passed June 1 — verify patching. CVE-2025-53770 (first reported in the March 6 brief) is now confirmed by GTI as the initial access vector for a China-nexus espionage campaign that also abuses ADCS for lateral movement.
CVE-2024-55591 / CVE-2025-24472 / CVE-2026-1731 / CVE-2025-10035	Fortinet FortiOS and FortiProxy; BeyondTrust RS/PRA; Fortra GoAnywhere	Various	AA26-222A; AA25-071A	Yes	Gunra and Medusa initial access vectors. Patch, then hunt for the forticloud-sync account and audit every RMM tool in the estate.
CVE-2025-66376 / CVE-2026-25089 / CVE-2026-39808 / CVE-2026-58644 / CVE-2026-48558	Zimbra Classic UI; FortiSandbox; SharePoint; SimpleHelp RMM	Various	AA26-204A; CISA KEV	Yes	Carried KEV and advisory items — confirm remediation and hunt where exploitation predated listing.
CVE-2026-0611 / CVE-2026-43994 / CVE-2024-12248 / CVE-2025-0626	Spacelabs Sentinel; coturn (telehealth); Contec CMS8000 monitors	9.8 / 8.1 / 9.8	June briefs; FDA / CISA	Yes / N/A	Patches available for Sentinel and coturn — confirm deployment. Contec FDA disconnect recommendation remains in force.

Threat Metrics

Activity Trends	Key Numbers This Week
▲ Clinical integration layer under advisory: the HL7 engine that holds downstream system credentials is now a disclosed attack surface ▲ DICOM advisory run reaches a fifth distinct product line (Orthanc), spanning libraries, viewers and now servers ▲ Second consecutive week with a GTI operation record confirming a US healthcare victim (UNC7072 CLOUDHAZE) ▲ Medtech cyberattack financial impact quantified: full-year guidance withdrawn following an August intrusion ▲ Virtualisation used for evasion: QEMU VMs for SSH port forwarding places traffic outside host monitoring	2 new CISA medical advisories on September 10 — both affecting core clinical data infrastructure 3 CVEs in Mirth Connect ≤ 4.7.1; one requires NO privileges (CVE-2026-82578, CVSS v4.0 8.7) 103 ATT&CK techniques mapped to CAMP.26.131 — among the broadest footprints in this series 21 new GTI-verified IOCs across 6 records — a low-volume week following last week's 3,781 Boston Scientific: Q3 AND full-year 2026 sales growth and adjusted earnings guidance now unlikely to be met CVE-2026-3650 (GDCM): NO PATCH — week 25; CVE-2026-56445 and CVE-2026-18844: NO PATCH



Activity Trends	Key Numbers This Week
► Vendor and third-party breaches continue to dominate healthcare disclosure volume	

Sources: Google Threat Intelligence (GTI), CISA ICS Medical Advisories ICSMA-26-253-01 and ICSMA-26-253-02 (September 10, 2026) and -225-01, -223-01, -223-02, -218-01, -216-01, -181-01, -176-01, -176-02, -083-01, CISA ICS Advisory index, CISA KEV Catalog, Joint Cybersecurity Advisories AA25-071A, AA26-222A, AA26-231A, AA26-237A, NVD / CVE Program / MITRE, OpenCVE, NextGen Healthcare, Orthanc, Boston Scientific (SEC filing), Veradigm, The Register, BleepingComputer, HIPAA Journal, PrivacyGuides Data Breach Roundup, BankInfoSecurity