Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical FileCatalyst Workflow Flaw Enabling Attackers to Gain Admin Access

Date of Publication	Admiralty Code	TA Number
August 29, 2024	A1	TA2024333

Summary

First Seen: July 2024
Affected Products: Fortra FileCatalyst Workflow
Impact: Fortra has patched a critical security vulnerability affecting its FileCatalyst Workflow software, identified as CVE-2024-6633. This flaw could be exploited by a remote attacker to gain administrative access to the system. CVE-2024-6633 arises due to the use of a static password to connect to an HSQL database, which is hardcoded into the software.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-6633	Fortra FileCatalyst Workflow Insecure Default Vulnerability	Fortra FileCatalyst Workflow	✗	✗	✓

Vulnerability Details

#1 Fortra has issued a warning about a critical security flaw in FileCatalyst Workflow, identified as CVE-2024-6633. This vulnerability has a CVSS score of 9.8 and could allow attackers to gain unauthorized access to an internal database, leading to data theft and privilege escalation to an administrator level. The flaw stems from the use of a static password to connect to an HSQL database, presenting a significant security risk.

#2 CVE-2024-6633 was discovered on July 1, 2024, due to the use of the same static password, "GO****GO***," across all FileCatalyst Workflow deployments. The vulnerability is particularly dangerous because the internal Workflow HSQLDB (HyperSQL Database) is remotely accessible via TCP port 4406 under the product's default settings.

#3 An unauthenticated local network attacker can exploit this vulnerability by accessing the internal HSQLDB using a remote JDBC URL (e.g., jdbc:hsqldb:hsql://<target-host>:4406/hsqldb). Once connected, the attacker can perform unauthorized operations within the database, such as adding an admin-level user to the DOCTERA_USERS table. This would grant them administrator access to the Workflow web application, enabling a range of malicious actions, including data theft and further system compromise.

#4 The HSQL database included with FileCatalyst Workflow is deprecated and intended only for installation and testing purposes; Fortra recommends switching to other supported databases. Upgrade to FileCatalyst Workflow version 5.1.7 or later or move away from depreceated HSQL database. Additionally, HSQL deployments can enhance security by restricting access to TCP port 4406 or disabling remote database access when feasible.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-6633	FileCatalyst Workflow 5.1.6 Build 139 (and earlier)	cpe:2.3:a:fortra:filecatalyst_workflow:*:*:*:*:*:*:*:*	CWE-200

Recommendations

Update: Users are recommended to upgrade to FileCatalyst Workflow version 5.1.7 or later to address the critical security vulnerability CVE-2024-6633. This update removes the use of a static password for the HSQL database connection, thereby mitigating the risk of unauthorized administrative access.

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit the vulnerabilities, providing an additional layer of protection.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0003 Persistence	TA0004 Privilege Escalation	TA0006 Credential Access
TA0040 Impact	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation
T1136 Create Account	T1552 Unsecured Credentials	T1565 Data Manipulation	T1565.001 Stored Data Manipulation

Patch Details

All users of Fortra FileCatalyst Workflow are strongly recommended to upgrade to version 5.1.7 or later. This update mitigates the risk associated with the static password flaw and is essential for maintaining the security of the system.

Link: https://filecatalyst.software/workflow.html

References

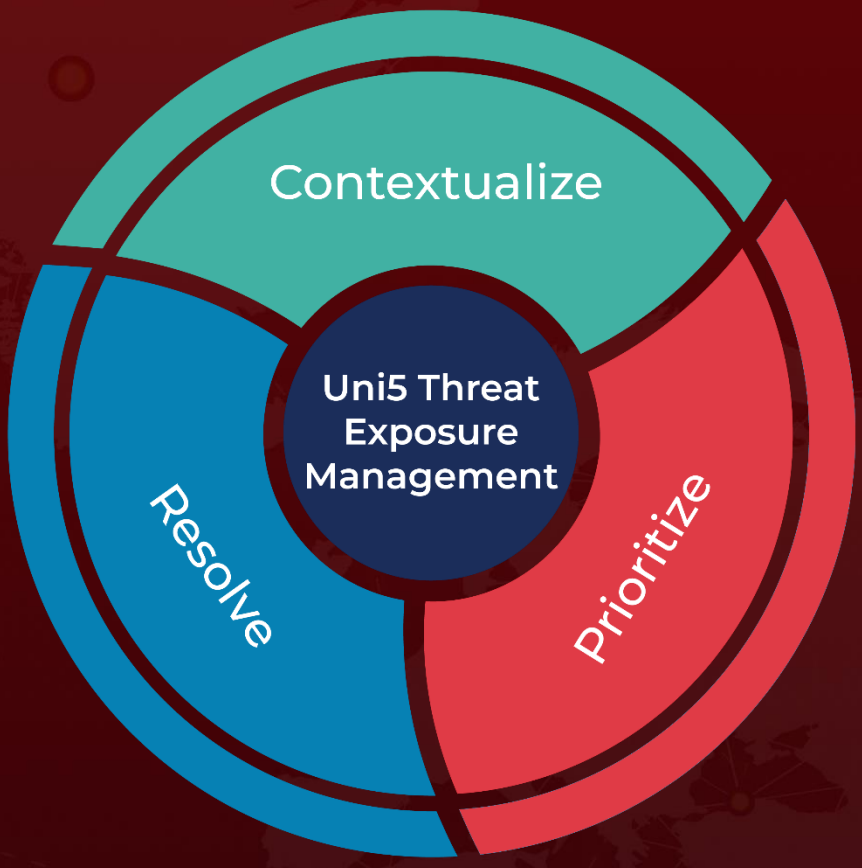
https://www.fortra.com/security/advisories/product-security/fi-2024-011

https://www.tenable.com/security/research/tra-2024-35

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 29, 2024 • 6:00 AM

More at www.hivepro.com