The DNAForge Vulnerability (v.2026-08-01)

A serious vulnerability has been identified in forensic DNA data files commonly used in criminal investigations, prosecutions, paternity/kinship testing, identification of human remains, cell-line authentication, and national defense. The affected file types are **.fsa** and **.hid** files.

Genetic analyzers produce .fsa and .hid files, which contain DNA signal data from fragment analysis of short tandem repeat (STR) regions. Signal data are interpreted, resulting in the generation of DNA profiles. These profiles are developed from evidence items (e.g. body fluids, human remains, swabs of items), and individuals' reference profiles. After profiles have been generated, comparisons can be made between evidence and/or reference profiles. These comparisons can be done manually by laboratory personnel or by automated databases, such as the U.S. Combined DNA Index System (CODIS) and similar systems in use by 70 member nations of Interpol.

The vulnerability is that these signal data can be **modified, swapped, or fabricated** after the file is created, affecting the interpretation-comparison process. Tampered files behave normally in commonly used forensic DNA software without warning the user that the underlying data has been changed. File headers containing metadata and analysis results can also be fabricated, allowing false signal data to be presented alongside false timestamps, false machine records, and false quality control data.

The vulnerability affects file formats that have been widely used in forensic DNA laboratories for approximately 30 years. A person with forensic DNA knowledge, but without specialized programming skills, can trivially modify files using the tool we created. The core issue does not invalidate DNA testing results. Rather, the issue is that **the data files currently produced during testing are not tamper-evident once they leave the instrument and are stored in or transferred between systems**.

Ultimately, we request that producers of genetic analyzers and laboratories achieve the same level of security for these digital artifacts as is given to physical evidence.

Why does this matter?

Forensic DNA evidence is often treated as highly reliable and can play a decisive role in criminal cases, military investigations, intelligence work, and identification of human remains. If the underlying data files can be altered without detection, the integrity of downstream DNA analysis may be compromised.

This matters for several reasons:

First, **.fsa and .hid files may be trusted too heavily in isolation**. If a laboratory, court, analyst, or outside reviewer receives only the file and not a secure record proving it is unchanged from the moment of creation, there may be no reliable way to confirm the file is authentic.

Second, the vulnerability can affect both raw signal data and associated analysis data. Tampering can alter the appearance of a DNA profile, simulate a mixture of multiple contributors, or add or remove apparent contributors from a sample.

Third, commonly used analysis programs do not flag these modifications. The modified files are accepted by several forensic DNA software tools, and internal checksum fields did not appear to prevent analysis or clearly alert users to tampering.

Finally, the consequence of tampering with files is severe. Tampering could affect all areas where DNA evidence is relied upon, including criminal justice, military/intelligence operations, and human

identification work. Any organization handling these files should assume risk until its systems and procedures are reviewed.

What can I do?

Organizations should not rely on .fsa or .hid files alone as proof of data integrity. The most important mitigation is to make files **cryptographically verifiable and tamper-evident** from the moment they are created.

Recommended actions include:

- **Implement cryptographic signing.** Genetic analyzers, collection computers, and laboratory systems should digitally sign files at the point of creation using hardware-backed private keys. This should include contextual information about how and where the files were generated. Public keys can then be used later to verify that a file is unchanged.
- **Use secure digital chain-of-custody controls.** Laboratories should document where files are created, stored, transferred, reviewed, and exported. File access should be logged and limited to authorized personnel.
- **Create trusted file snapshots.** Laboratories should store cryptographic hashes or other integrity records in a secure Laboratory Information Management System, or LIMS, as soon as files are generated.
- **Verify files before analysis or disclosure.** Any file used in criminal, civil, defense, research, or intelligence contexts should be checked against a trusted integrity record.
- **Review existing laboratory protocols.** Laboratories should assess whether their current systems protect files during transfer from instrument to computer, from computer to server, from server to LIMS, from the lab to outside parties, as well as anytime the files are at rest.
- **Treat legacy files carefully.** Older files may not have reliable integrity records. Where possible, they should be evaluated alongside chain-of-custody documentation, laboratory records, instrument logs, analyst notes, and independent corroborating evidence.

FAQs

Does this mean forensic DNA testing is unreliable?
No. The concern is not that DNA science is inherently unreliable. The concern is that certain DNA data files may be vulnerable to undetectable tampering after they are created.

Are all .fsa and .hid files compromised?
No. The disclosure identifies a vulnerability, not proof that any specific file has been altered. However, files should not be trusted in isolation unless their integrity can be verified.

How much of forensic DNA testing is vulnerable?
Most of it. The .fsa file format has been used by capillary electrophoresis instruments, which have been used for the vast majority of forensic DNA testing since the late 1990s.

Who may be affected?
Criminal defendants, victims, forensic DNA laboratories, prosecutors, defense attorneys, courts, military and intelligence agencies, paternity-testing organizations, researchers, and anyone relying on .fsa or .hid files for DNA interpretation in specific cases may be affected. The general public is affected by any resulting loss of confidence in the justice system if scientific evidence is admitted without authentication or demonstrations of resistance to tampering.

Can tampering be detected?
Sometimes, but only if there is a reliable preexisting integrity record, such as a cryptographic hash, secure LIMS snapshot, digital signature, or strong chain-of-custody documentation. Internal technical review and external expert review alone are unlikely to detect altered data.

What is the best long-term fix?
The best long-term fix is hardware-level cryptographic signing at file creation, combined with strong laboratory information management, access controls, audit logs, and routine file-integrity verification.

Should these files be encrypted?
Encryption protects confidentiality, but it does not automatically prove authenticity and may limit independent inspection. The better approach is tamper-evident digital signing, performed by both the source hardware and the producing laboratory, which allows for data verification without compromising data transparency.

Are only US files subject to this vulnerability?
No. The vulnerability is due to the file formats, not the geographic origin of the data. All laboratories producing .fsa or .hid files should take precautions to guard against this vulnerability.

Has the vendor responded?
Yes, on July 31, 2026, the vendor issued a security bulletin that includes links to software patches for affected systems. This response should be considered by stakeholders as they determine their own responses to this vulnerability.

Authors

Nathaniel Adams, Systems Engineer, Forensic Bioinformatic Services, Inc.
Laura Gaydosh Combs, Ph.D., Associate Professor of Forensic Science, Henry C. Lee College of Criminal Justice and Forensic Sciences, University of New Haven
Kevin P. Dyer, Ph.D., Security Engineer
Dan E. Krane, Ph.D., Professor of Biological Sciences, Wright State University

Contact Information

For questions or further information regarding this vulnerability, please contact Nathaniel Adams at DNAForge.CVE@gmail.com.