

— SECURITY / 16 MIN READ

Every Company Has an fbijobs.gov

Oracle's patch was out for three and a half months. The firewall workaround many organizations used instead could be bypassed by changing one character.

WRITTEN OCTOBER 8, 2026 • UPDATED OCTOBER 25, 2026

KEY TAKEAWAYS

01

The FBI says a contractor failed to apply a patch Oracle had issued in June. Many organizations relied on a firewall rule instead, and attackers got past it by changing one character in the request.

02

The portal was planned to the lowest of three federal control baselines, the level suited to a careers site, yet officials say the leak covers nearly every FBI employee. Classify systems by what they can reach, not what they are for.

03

A vendor running the system leaves the risk with you. Hold vendors to your own patching standard, ask for evidence, and go find your own fbijobs.gov: the vendor-run portal with real data that nobody watches.

Security is only as strong as its weakest link, and the recent FBI breach proves it. The FBI was attacked around September 21 by a group known as ShinyHunters, and, according to Reuters²¹, the attack went through the Oracle PeopleSoft software that runs the FBI job application portal, fbijobs.gov. The FBI has since said a contractor failed to apply a security patch issued to protect the platform. This piece goes through what is publicly known, what is only claimed by the attackers, and what any organization that runs a vendor-supplied portal should take from it. PeopleSoft is Oracle's HR software, the kind of system that stores job applications, employee records and benefits, and the FBI, like many large organizations, uses it behind its careers website. According to anonymous FBI officials, the attackers did not reach the bureau's investigative or classified networks, but the HR side turned out to hold almost as much sensitive information about agents as anything else would.

A quick recap of the dates first, because the timing is the whole story here. Everything is 2026, and where it is only the attackers saying it, it is marked as such.

- May 15 is when the FBI puts out the advisory about ShinyHunters through IC3 (PSA260515) about how they extort people, the calls to family members, the swatting. This is the advisory the group later says is the reason they went after the FBI.
- Twelve days later, May 27, the same group is already exploiting a PeopleSoft zero-day, mostly against universities at that point, and there is no patch for it.
- June 10 Oracle ships the patch for the bug (CVSS 9.8). Oracle's stopgap for anyone who cannot patch right away is to switch off or remove the vulnerable component, with blocking the endpoint at the firewall as the fallback. Same day the University of Nottingham confirms its student records got taken, around 454,600 people per Have I Been Pwned.
- Then the important gap. Three and a half months where the patch exists and, at the time, nothing is said publicly about the FBI portal. Reuters has not been able to determine whether or when those responsible for the portal followed Oracle's advice.
- September 15 the Dutch police, together with the FBI, arrest a 24-year-old in Amsterdam who they say is part of the group. The group denies he is one of theirs.
- September 21 by their own account ShinyHunters are inside the FBI jobs portal, September 22 the site is defaced and the portals go offline. Over the next three days samples on about 5,000 people go out to journalists; Reuters, 404 Media and the BBC are able to partly verify them, and Reuters verifies the details of more than 20 people in the samples.
- September 25 is also the day Mandiant publishes that the firewall workaround can be bypassed by changing one character and that they are finding web shells on

dozens of systems. There are no reports of fully patched systems being compromised.

- End of September Reuters reports an internal FBI memo that assumes everyone's data is out, ShinyHunters say they will not publish and drop their deadline, a second alleged member gets picked up in Jordan and the group's dark-web leak site goes offline.
- October 6 the FBI says a contractor "failed to implement a security patch explicitly issued to secure the platform" and that it has removed the contractor. Reuters, citing two sources, reports the platform was PeopleSoft and the contractor came from Accenture.
- October 9 FBI Director Kash Patel announces the arrest of another suspected co-conspirator, without naming him. Court records and press reports identify the man arrested in Pennsylvania on October 8 as Edward Dubrovsky, a 54-year-old Canadian cybersecurity executive who until December 2025 was a managing director at a ransomware negotiation firm. The FBI has not said whether he is the person Patel meant. According to court records cited by KrebsOnSecurity he is charged with conspiring to threaten the release of stolen data to extort money, and with interfering with commerce by threats. The complaint is sealed, and he has not been convicted.
- October 19 KrebsOnSecurity reports that investigators have found unusually close ties between ShinyHunters and executives at two ransomware negotiation firms, including a U.S. executive who allegedly helped run the group's Shinywire.com extortion site, which went offline on October 16. That executive has not been named or charged.
- October 25, as of the latest update, there is still no Oracle advisory for any new zero-day. Oracle's quarterly update on October 20 fixed other PeopleSoft flaws; none has been reported as exploited. The FBI has not said which patch was missed or whether a firewall rule was all that stood in its place.

What is a zero-day?

A zero-day is a security hole that attackers are using before the vendor has a fix for it, so defenders have had "zero days" to prepare. Once Oracle published a fix on June 10 it stopped being a zero-day and became a known, patchable bug. CVSS is the standard 0 to 10 severity score; 9.8 is about as bad as it gets, meaning an attacker who can reach the vulnerable component can take over the server without a password.

01 The vulnerability

The zero-day campaign ran from May 27 to June 9. ShinyHunters started by attacking mostly universities through CVE-2026-35273, with financial and health care institutions showing up among the victims in the later wave. The security alert for the CVE, with a CVSS score of 9.8, went out on June 10, when Oracle provided a patch to fix the vulnerability. Mandiant's guidance for anyone who could not patch right away was to block the vulnerable endpoint at the firewall. The bug is a Java deserialization flaw (the software trusts a package of data it should not) in the PeopleSoft Environment Management Hub, an administration component that lives on the web server at /PSEMHUB/hub and accepts requests without any authentication. It is supposed to only be reachable from inside the organization, but in a lot of deployments it ended up exposed through the same reverse proxy as the public site, and on those systems anyone on the internet who found it could run their own code on the server, which security people call remote code execution.

However, after the advisory went live it seems many IT teams decided to apply the firewall stopgap only. On September 25 Mandiant reported that the firewall stopgap, as many organizations had written it, could be bypassed by changing one character in the request. Instead of /PSEMHUB/ the attackers request /%50SEMHUB/, where %50 is just the letter P percent-encoded. A rule that compares the raw text of the request does not see a match, then the WebLogic server behind it decodes the P and routes the request to the vulnerable component anyway. Mandiant found web shells on dozens of systems and says the organizations being targeted were the ones that had put in the firewall rule and not the patch.

How one character beat the firewall

Think of the firewall rule as a bouncer with a list that says "nobody gets in asking for PSEMHUB." The attacker writes the name as "%50SEMHUB" instead. The bouncer compares it letter by letter, does not see a match and waves them through. The receptionist inside (the application server) knows that %50 is a valid alternative way of writing the letter P in a web address, translates it, and sends them straight to the room the bouncer was supposed to be guarding. Better firewalls translate before they compare; the rules many teams wrote did not. A web shell is what the attacker leaves behind once inside: a small hidden page that lets them come back and run commands whenever they want.

02 The attack on the FBI

ShinyHunters claim that they compromised fbijobs.gov on September 21 and by September 22 they had defaced it. They say they then pivoted to the AWS environment where applicant and employee data is stored and took somewhere between 2 and 3 TB. They also say they got into BEAST, which is the FBI system for background checks, MedLink which has the medical records, and one of the criminal justice systems. None of that can be verified from outside the FBI. Officially the FBI has confirmed the intrusion and said the incident "involved a failure of a platform managed by a third-party vendor"; officials speaking anonymously have added that the classified and investigative networks were not touched, and nothing verified so far contradicts that.

At first ShinyHunters were saying it was a new PeopleSoft zero-day. A few days later they told BleepingComputer that against the FBI they used the same one-character firewall bypass, but they still say there is a second bug in the same component that nobody knows about. Maybe. There is no way of knowing from the outside, but as of today Oracle has not published anything new and has not issued another CVE, and Oracle's own mitigation guidance names more than one way into that component, so until something changes the working assumption here is the known vulnerability and the known bypass. That is the boring answer, and in these cases the boring answer is usually the right one. The FBI's October 6 statement that a contractor missed a patch points the same way.

On what was actually leaked, the FBI has not published a list, so what exists is what the journalists were able to verify from the samples plus what current and former people at the FBI have told the press. Everything you would expect from an HR system is in there: name, SSN, date of birth, home address and emergency contact, plus the employee ID and what the person actually works on. Reuters also reported medical and psychiatric records in files it reviewed. The job assignment is the part that should bother people most, because a foreign intelligence service does not care that much about the SSN of an agent, it cares that it now knows who in a given field office works the cartel cases and where that person lives, who is doing HUMINT, who is in electronic surveillance, and who sits in the Remote Operations Unit, which is the group that builds the FBI's own offensive tooling. According to [six current and former FBI officials who spoke to MS NOW](#)⁹, this covers nearly every FBI employee (the bureau employs roughly 38,000 people), plus more than 8,000 state and local officers who sit on FBI

task forces. The attackers say job applicants are in it too. The sensitive-role detail comes from Reuters, which analyzed the sample on September 23, and from Nextgov/FCW, which reviewed it as well. People are comparing it to the 2015 OPM breach, the theft of background-investigation files on about 21.5 million people, widely attributed to China. The comparison seems fair.

Some people have guessed that this was a nation state, but the evidence points the other way. The group defaced the site, they went to the press, they wrote an open letter to the FBI director asking for the May advisory to be taken down, and nothing that has come out so far suggests they asked the FBI for money, which for a crew the FBI says has collected over 70 million dollars in extortion is a strange way to behave unless the advisory really was the point. Three people have now been arrested: one in the Netherlands, who the group says is not one of theirs; one in Jordan, who according to Reuters is cooperating with the FBI; and a Canadian in Pennsylvania in October, whom press reports tie to the group. A state operation does not normally end with its people getting picked up within weeks. The usual state actor would have gotten in, taken the data quietly and the FBI would have found out two years later if ever. There are exceptions, states have hidden behind noisy personas before, Guccifer 2.0 and the Sony hack being the obvious ones, and some analysts do not rule out a state hand in the timing or in where the data ends up, but nobody has named a country and the arrests point at a criminal crew. In a way that is the more uncomfortable version, since it means it did not take a nation state to do this.

03 Three and a half months

The surprising fact is that the patch was available for three and a half months. The FBI has since confirmed the outline: a contractor "failed to implement a security patch explicitly issued to secure the platform." It has not said which patch, and the most likely explanation from what is public is that whoever ran the job application portal relied on a workaround or a partial fix rather than the full patch. One FBI cyber agent told MS NOW it was "definitely incompetence", describing "a vulnerability that supposedly they thought they patched, but managed to miss one of the ways to patch it."

The FBI's statement settles what was guesswork until October 6: patching the portal was a contractor's job, so this was not a managed service where Oracle applies the updates. The FBI's own privacy impact assessment from 2022 says the Candidate Gateway runs PeopleSoft HRS 9.2 on AWS GovCloud, is "accessible from the Internet", and

passes applications daily to an internal system called HR Source. That means Oracle is not applying the patches, whoever manages that instance is. The same document rates the system "Medium" under FIPS 199, yet says its NIST 800-53 control baseline was "anticipated to be at the LOW impact level," the lowest of the three. That is the sort of designation given to a careers website, not to a system that would end up being the way in to the personal details of FBI agents.

The 2022 design is also interesting for what it says about the data. On paper, HR Source sits on the FBI's classified network, the portal talks to it only through one-way cross-domain guards, and applicant data is purged from the portal automatically, though only after up to a year. If that was still the architecture in September, the portal should have held at most a year of applicant records, not files on the whole workforce, and the attackers' story about pivoting into the HR systems gets harder to believe. The samples the journalists verified say otherwise, so either the design changed or data that belonged on the inside had been copied to the internet-facing side.

Who patches a vendor-run system?

"Managed by a third-party vendor" can mean very different things. With true software-as-a-service the vendor runs everything and patches it for you. With software you install yourself, even in a cloud like AWS GovCloud, the vendor only publishes the fix and your own team or your contractor has to apply it. The FBI's own 2022 paperwork describes the second model, so if the patch was not fully applied, that was the job of whoever operates the portal on the FBI's behalf, not Oracle's.

The FBI has highly talented cybersecurity engineers helping protect not only its own infrastructure but that of many other institutions. One thing that happens all the time, and it is a guess whether it happened here, is that the HR or hiring department decided to use an external tool, it was validated at the time, a vendor was contracted to run it, and then nobody treated it as a system that holds the home address of every agent in the country, because on paper it was a careers website. The same FBI agent put it more bluntly to MS NOW, that the data belonged on an internal system and somebody moved it all onto one that faced the internet, which would square with the gap between the 2022 design and what actually leaked. Either way the system that gets you is usually the one nobody considered important enough to worry about.

04 The problem with closed source

The problem with software like PeopleSoft is that it is closed source, meaning outsiders cannot read its code, and sits behind a paywall. Even basic documentation on the vulnerable component is hard to come by outside Oracle's support portal, and that is a recipe for disaster when the component is sitting on the internet. A closed-source app exposed to the internet is an attractive target. Secret code is somewhat harder to attack, but fewer outsiders have reviewed it, and it probably gets independent audits less often.

To be fair, this is not a clean argument. This particular bug was also reported by outside researchers through TrendAl's Zero Day Initiative, a third-party program that does pay, though ZDI dates its report to June 10¹⁸, the day the patch shipped and two weeks after ShinyHunters began exploiting it. And open source has had its own disasters, Log4Shell being the obvious one. Open source is not a guarantee of anything. The point is narrower: when the code is closed and the vendor does not pay for bugs, the people looking at it are mostly the ones who intend to use what they find.

Additionally, Oracle does not maintain a public, paid bug bounty program (a standing offer to pay researchers who report security holes responsibly, so that reporting pays better than selling the bug to criminals); the only thing they offer is public credit in the advisory. Their own FAQ says "Oracle does not maintain an open bug bounty program at this time." Not surprisingly, the incentives are misaligned. A whitehat has less reason to spend weeks taking apart software whose vendor does not pay, while a blackhat's payoff for the same work can be large. In this case it was access to the FBI. It is worth noting that ShinyHunters were already exploiting this vulnerability in the wild when Oracle's alert came out.

05 Lessons

The first lesson is to have a good reason when considering adding a third-party tool, and when you do, consider 1) if it is necessary, 2) if it is open source and 3) if the vendor has a public bug bounty program that pays. None of those is a guarantee of course, but at least you know that people outside the vendor have looked at the code and that they have a reason to tell the vendor when they find something instead of selling it.

Beyond that, a few more things to take from this incident:

- Patch, do not rely on the firewall rule. Mandiant says the organizations being hit in September were the ones that had done the firewall rule and skipped the patch, and by the FBI's own account its breach came down to a patch its contractor never applied.
- If you really have to live with a firewall or WAF rule for a while, make sure it decodes and normalizes the URL before it matches, otherwise one encoded character is enough, which is what Mandiant found across dozens of victims.
- Admin and management endpoints like the Environment Management Hub should not be reachable from the internet at all, Oracle itself intends that component for internal addresses only, and the same goes for any admin endpoint on any product.
- The applicant portal should not be able to reach the HR system of record, and the FBI's 2022 design actually got this right on paper. The question is what changed between the paperwork and September, because a site for job seekers ended up within reach of the medical files of current agents. A public front end and your most sensitive data should not share the same blast radius (the set of systems an attacker can reach once inside one of them), and the architecture diagram is only worth anything if someone checks it is still true.
- Vendors managing a platform for you should be held to your own patching standard and should show you evidence of it. "Managed by a third party" does not say anything about who was responsible.
- Classify systems by what they can reach, not by what they are for. A careers site rated LOW impact is reasonable right up until it is wired into the HR system of record.
- If the terabytes claim is anywhere close to true, that is a lot of data leaving an AWS environment without anyone noticing, so monitor what leaves: watch for unusually large transfers out of your network.
- And finally, the FBI published an advisory about this group in May, four months before the breach. That should have been the trigger to go over every internet-facing system they own, and the outcome suggests that either did not happen or did not catch this one.

Most companies have their own fbijobs.gov somewhere, some portal that HR or sales or finance bought a few years ago, a vendor runs it, it has real customer or employee data in it, and the security team does not spend much time on it because it is not the main product and it was rated low risk when it was bought. It is worth going and finding that system, checking when it was last patched, what parts of it are exposed to the internet, and what else it can reach once somebody is inside it, because that last question is the one that, going by the outcome, nobody asked about the FBI portal until it was too late. ■

REFERENCES

- 01 www.oracle.com/security-alerts/alert-cve-2026-35273.html
- 02 www.ic3.gov/PSA/2026/PSA260515
- 03 www.fbi.gov/file-repository/pias/pia-fbijobs-fbicg-100322...
- 04 www.oracle.com/corporate/security-practices/testing/faq/
- 05 www.bleepingcomputer.com/news/security/shinyhunters-uses-...
- 06 www.bleepingcomputer.com/news/security/shinyhunters-claim...
- 07 www.bleepingcomputer.com/news/security/nottingham-univers...
- 08 www.trendaisecurity.com/en-us/resources-insights/trendai-...
- 09 www.ms.now/news/fbi-hack-shinyhunters-breach-data
- 10 www.nextgov.com/cybersecurity/2026/09/shinyhunters-says-i-...
- 11 krebsonsecurity.com/2026/09/dutch-police-arrest-reformed-...
- 12 www.cbsnews.com/news/shinyhunters-hacker-detained-jordan-...
- 13 www.reuters.com/world/hacked-fbi-data-has-sensitive-infor...
- 14 www.reuters.com/world/middle-east/key-shinyhunters-hacker...
- 15 www.foxnews.com/us/fbi-strikes-back-hacking-group-oversea...
- 16 www.zerofox.com/intelligence/shinyhunters-claims-breach-o-...
- 17 www.helpnetsecurity.com/2026/09/28/fbi-job-portals-offlin...
- 18 zerodayinitiative.com/advisories/ZDI-26-388
- 19 cloud.google.com/blog/topics/threat-intelligence/shinyhun...
- 20 cloud.google.com/blog/topics/threat-intelligence/shinyhun...
- 21 www.reuters.com/technology/accnture-contractor-removed-f-...
- 22 krebsonsecurity.com/2026/10/fbi-arrests-founder-of-ransom...
- 23 krebsonsecurity.com/2026/10/feds-suspect-ransom-negotiato...



Nonlinear Advisors
Steady hands for nonlinear growth.

info@nonlinearadvisors.com | nonlinearadvisors.com | [LinkedIn](#) | [X](#)

Nonlinear Advisors provides finance, operations, security and strategic advisory services. It is not a CPA firm and does not provide audit or attest services. It is not a registered investment adviser or broker-dealer, does not solicit investors, and does not receive transaction-based compensation. Nothing in this piece is legal, tax or investment advice. © 2026 Nonlinear Advisors LLC, New York.