

Forum:[Hack Forums](#)

Thread: [U.S. Puts \\$10M Reward on FSB Hackers Behind Cisco Exploit Targeting Critical Infrastr](#)

JoseMar - September 5, 2025, 8:06 pm

U.S. Puts \$10M Reward on FSB Hackers Behind
Cisco Exploit Targeting Critical Infrastructure

So the US is dangling \$10M for info on three FSB dudes who've apparently been running ops against critical infrastructure. Real names, real photos, plastered all over like they're wanted posters from the Wild West. Except instead of horse thieves it's guys popping Cisco gear with decade-old vulns.

Feels like the kind of headline you scroll past, but then it sticks in your head. Like... wait, ten million? For hackers?

Cisco Is The Punchline
It's always Cisco. Always.

Half the time it's because their stuff is so ingrained in infrastructure that ripping it out is basically impossible without blowing half the network up. The other half is because admins just... don't patch. "Mission critical" apparently translates to "don't touch anything ever."

The vuln here (CVE-2018-0171) is ancient. It's Smart Install protocol junk that should've been killed years ago. But nah, these boxes sit there humming along in substations, water plants, random factories, and nobody wants to risk downtime to update. So they stay exposed, like open wounds.

The FSB guys didn't need zero-days. They just needed patience and a scan button. It's embarrassing.

Elite Hackers or Persistent Skids?
This is the part that gets me. The media frames these state groups like Bond villains. But let's be real: half their playbook is just... exploiting lazy configs. End-of-life gear, default SNMP communities, no updates since Obama was in office.

That's not "advanced." That's persistence with a government paycheck.

Don't get me wrong, they're dangerous. Not because they're genius coders, but because they don't stop. They'll scan every dusty router on the planet until they get a foothold. And once they're in, they play the long game: backdoors, config changes, months of reconnaissance. It's slow, boring, effective.

Meanwhile, some skid brags on HF about running metasploit on his neighbor's WiFi like he's a god. These guys are in power grids. Different leagues, but not because of skill, because of scope.

That \$10M Question
Who's actually gonna cash in on this?

Think about it. If you're in Russia and you know these guys personally, snitching means you're either dead or disappeared before you ever touch that money. If you're outside Russia, good luck

even finding them.

So maybe the bounty isn't about really paying anyone. Maybe it's just noise. A way of saying "we know your names, we know your faces, and we're willing to pay big to screw with your lives." It's psychological warfare as much as cybersecurity.

Feels like a PR move, but also... it plants seeds. Someone, somewhere, with the right grudge might bite.

My Take and I finish here
I keep flipping between "lol, same old Cisco story" and "holy shit, this could actually take down a grid."

The depressing part is it's not new. These guys (Berserk Bear, Dragonfly, Static Tundra, pick your edgy codename) have been around for over a decade doing the same tricks. Exploiting the same weak points. Dropping malware that everyone already knows exists. And yet, still successful. Because nobody patches. Nobody budgets to rip out old hardware. Nobody cares until something breaks.

That's what makes them dangerous. Not some Oday arsenal. Just patience + systemic negligence.

Anyway, I doubt anyone here is sitting on FSB doxx, but it's an interesting shift. Governments treating hackers like terrorists, throwing bounty money around. Makes you wonder where this all heads in the next five, ten years.

And also... if Cisco ever just nuked Smart Install from orbit, half these headlines wouldn't even exist.

webdev77 - September 5, 2025, 8:20 pm

(Sep 5, 2025 08:06 PM)JoseMar Wrote: [\[CITE\]](#) Because nobody patches. Nobody budgets to rip out old hardware. Nobody cares until something breaks.

Because there's no real penalty for simply not giving a flying fuck about security. Why bother if the general public has simply accepted that all info is already out there and shareholders have already factored in being hacked a couple times into the valuation? Obviously a bit of an exaggeration here, but it's pretty clear that maintaining tight security is not valued all that highly for the vast majority of organizations in existence.