

9 June 2009

By: Lucian Constantin, Web News Editor



Low-cost VPS provider
hit by hackers via
0-day vulnerability
VAServ LLC

[VAServ Hack Results in Massive Data Loss](#)

Zero-day vulnerability in virtualization software exploited to delete server data

A 0-day vulnerability in HyperVM, a virtualization application produced by Lxlabs, led to a major hack on the servers of VAServ, a UK-based hosting provider. The attackers obtained root access and wiped large portions of the data.

VAServ is a low-cost virtual private server (VPS) provider serving thousands of customers. The company has servers located both in the UK and the US. On Sunday evening, unknown hackers exploited a vulnerability in the HyperVM software used by the company and obtained administrative permissions on its systems.

The perpetrators then proceeded to delete data from tens of UK and US servers. Company staff were alerted by the suspicious activity and intervened, but the damage was already done. They have since [been working](#) 24/7 to restore what they can, but it's likely that some of the data has been lost forever.

Rus Foster, the company's CEO, noted that about 50 percent of customers did not sign up for managed services, meaning they did not benefit from automatic backup. Those users might never be able to recover their data, unless they backed it up themselves.

This attack comes after last Thursday someone anonymously [published](#) exploit code for a staggering 24 high-risk unpatched vulnerabilities in the Kloxo software, also developed by Lxlabs. Kloxo Enterprise is a web-based central management platform with the ability to "manage 100s of thousands of domains on hundreds of servers," according to the vendor.

There is no confirmation yet, but it is likely that VAServ was also using this software for managing its HyperVM-based infrastructure and one of these publicly disclosed vulnerabilities represented the point of entry.

The unknown individual who disclosed these flaws claimed that the vendor was unresponsive to their reports. According to him, he originally notified Lxlabs on 21 May and received a confirmation from it. On 4 June, however, he wrote, "Nothing heard from vendor, and the private resource containing the vulnerability info still does not appear to have been accessed." This led him to conclude that the "vendor appears uninterested."

According to [The Register](#), Foster also attempted to contact Bangalore-based Lxlabs about the vulnerability, but did not receive any response. "I've heard from other people they've been hit by the same thing," he notes.

Meanwhile, Lxlabs' founder and owner, K T Ligesh, [was found dead](#) in his house yesterday, in what appears to be a case of suicide by hanging. His best friend reported that the night before he drank heavily and was depressed over losing an important contract and the suicide of his mother and sister five years ago.