Over 20,000 data center management systems exposed to hackers

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** January 29, 2022 11:08 AM **0**

Researchers have found over 20,000 instances of publicly exposed data center infrastructure management (DCIM) software that monitor devices, HVAC control systems, and power distribution units, which could be used for a range of catastrophic attacks.

Data centers house costly systems that support business storage solutions, operational systems, website hosting, data processing, and more.

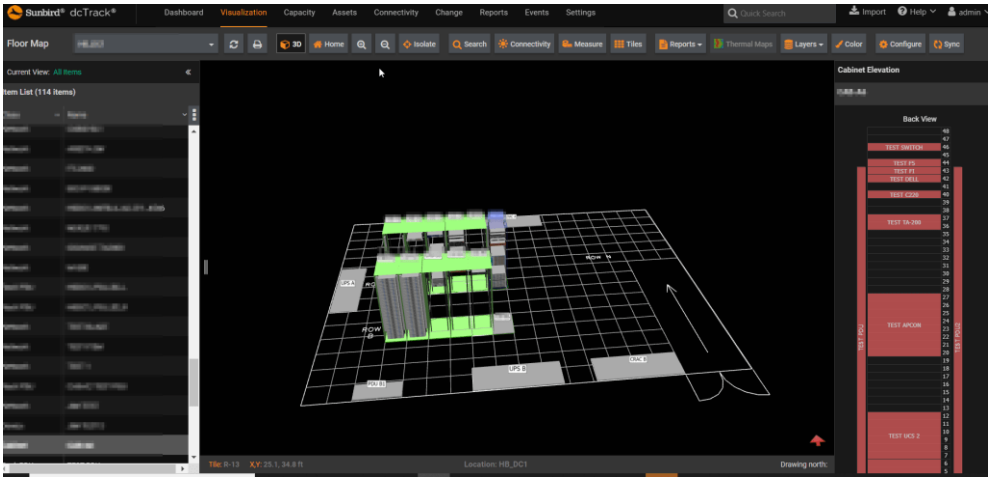
The buildings that host data centers must comply with strict safety regulations concerning fire protection, airflow, electric power, and physical security.

Years of pursuing operational efficiency have introduced "lights-out" data centers, which are fully automated facilities managed remotely and generally operate without staff.

However, the configuration of these systems isn't always correct. As a result, while the servers themselves may be adequately protected from physical access, the systems that ensure physical protection and optimal performance sometimes aren't.

Multiple cases of unprotected systems

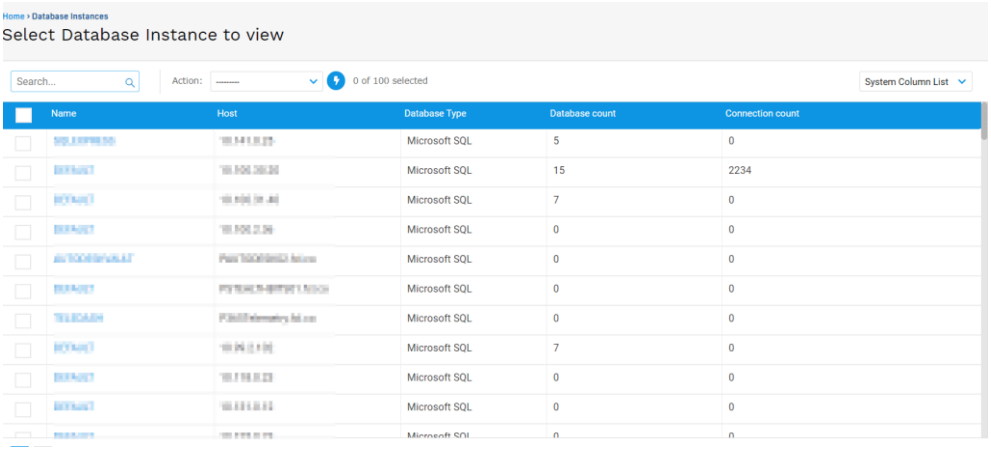
Investigators at Cyble have found over 20,000 instances of publicly exposed DCIM systems, including thermal and cooling management dashboards, humidity controllers, UPS controllers, rack monitors, and transfer switches.



Rack details on the exposed data center

Source: Cyble

Additionally, the analysts were able to extract passwords from dashboards which they then used to access actual database instances stored on the data center.



Databases accessed in second phase

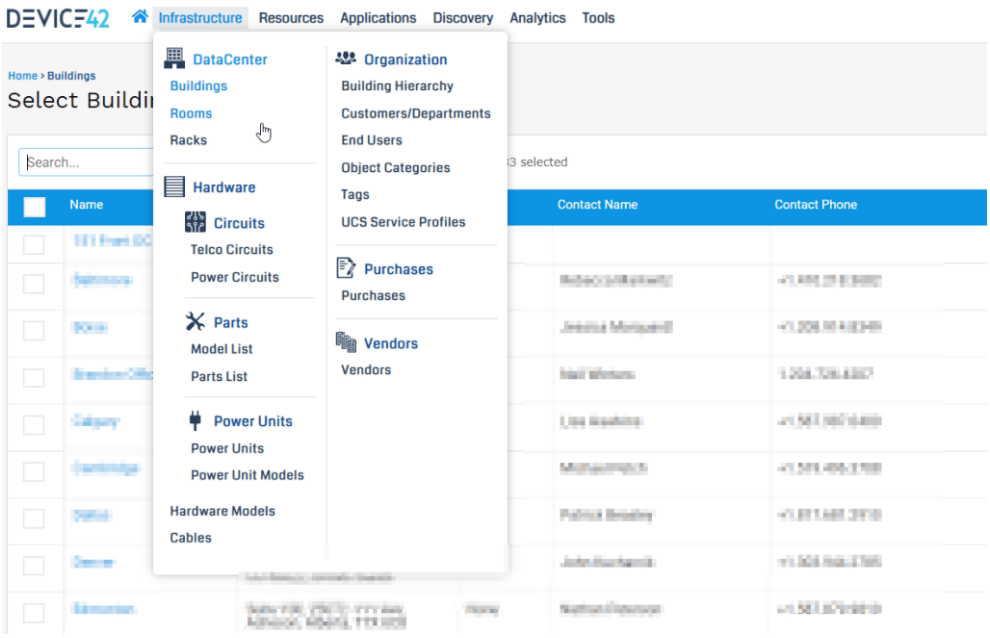
Source: Cyble

The applications found by Cyble give full remote access to data center assets, provide status reports, and offer users the capacity to configure various system parameters.

Sunbird dashboard

Source: Cyble

In most cases, the applications used default passwords or were severely outdated, allowing threat actors to compromise them or override security layers fairly easily.

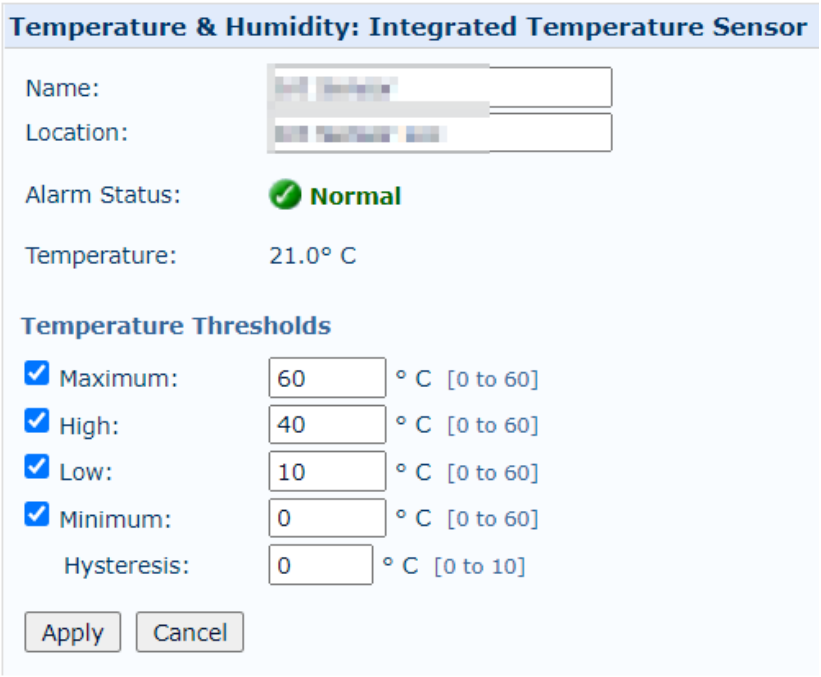


Device42 systems dashboard

Source: Cyble

Potential impact

Exposing these systems without adequate protection means that anyone could change the temperature and humidity thresholds, configure voltage parameters to dangerous levels, deactivate cooling units, turn consoles off, put UPS devices to sleep, create false alarms, or change backup time intervals.



Accessing temperature threshold settings

Source: Cyble

These are all potentially dangerous acts that may result in physical damage, data loss, system destruction, and a significant economic impact on the targeted organizations and their clients.

An example of this is a fire incident in the Strasbourg-based OVH data center in March 2021 (https://www.bleepingcomputer.com/news/security/ovh-data-center-fire-likely-caused-by-faulty-ups-power-supply/), caused by a failure in one of the building's UPS (uninterruptible power supply) units.

While that occurrence wasn't the result of hacking, it illustrates the magnitude of the damage that such attacks can cause to service providers and their customers.

The fire consumed thousands of servers, irreversibly wiped data, and caused service disruption to gaming servers, cryptocurrency exchanges, telecommunication firms, news outlets, and more.

Even if no physical harm is done, adversaries can use their access to DCIM systems to exfiltrate data or lock the real admins out and eventually extort the data center owner.

The implications, in any case, are dire, and closing these loopholes should be a priority. On that front, Cyble has informed the CERTs on each country where the exposed systems were located.

Over 20,000 ILO interfaces exposed as well

In addition to exposed DCIM instances, security researcher and ISC Handler Jan Kopriva (https://twitter.com/jk0pr) found over 20,000 servers with exposed ILO management interfaces (https://isc.sans.edu/diary/28276).

HPE Integrated Lights-Out (iLO) management interfaces are used to provide remote low-level access to a server, allowing administrators to remotely power off, power on, reboot, and manage servers as if they were physically in front of them.

However, if not correctly secured, threat actors will now have complete access to servers at a pre-boot level, allowing them to modify the operating system or even hardware settings.

Like DCIM interfaces, it is critical to secure ILO interfaces properly and not expose them directly to the Internet to protect them from remote exploitation of vulnerabilities and password brute force attacks.