Weekly roundup: third-party breaches, exposed dashboards and an unpatched Windows lock screen bypass



SecurityWeek's weekly roundup covers a vendor-led breach at Infoblox, a Fugaku supercomputer intrusion via a public dashboard, a test-environment breach at Rakuten Securities, and an unpatched Windows 11 lock screen bypass.

- Infoblox confirmed attackers reached company data through a compromised data migration vendor; some customers' NIOS configuration snapshots were reportedly among the stolen files.
- Riken suspended the Fugaku supercomputer after an outside party used a public status dashboard to enter its internal operations network.
- Rakuten Securities said an intrusion into a test environment on November 11 may have exposed data on millions of accounts.

> - Researcher Nightmare Eclipse published FastUnlock, an unpatched Windows 11 flaw that abuses Narrator to bypass the lock screen; it needs physical access.
> - Equinor stopped an attack on some IT systems with no impact on production, and Skagerak Energi reported a possible attempted intrusion.

SecurityWeek's weekly roundup gathers several incidents that offer practical lessons for security and risk teams. Three of them share a theme: exposure through assets that organizations often treat as low risk.

Third parties, test systems and public dashboards

Infoblox confirmed that attackers accessed certain company information through a compromised third-party data migration vendor. Media reports cited in the roundup say the vendor handled SharePoint migration and that the stolen files included NIOS configuration snapshots for some customers, along with personal details of employees and their dependents. Infoblox says it has no indication that its products, cloud services, software updates or build-and-release processes were involved.

In Japan, Riken suspended the Fugaku supercomputer and cut off external access. It said an outside party used a public dashboard showing the system's operational status to break into the internal operations network and tamper with several servers. Names, email addresses and user IDs of up to 4,597 users may have been exposed.

Rakuten Securities said attackers accessed a test environment system on November 11. Login IDs and branch codes for up to 11.25 million accounts, and personal and financial details for up to 4.47 million accounts, may have been exposed.

Other items to note

Researcher Nightmare Eclipse published FastUnlock, an unpatched Windows 11 zero-day. It abuses the Narrator screen reader to get past the lock screen and run code as the lock screen account. It requires physical access and at least one account linked to an online Microsoft account.

Equinor said it stopped an attack on some IT systems detected on November 17, with no effect on production and no sign of data theft or alteration. Skagerak Energi reported possible attempted intrusion activity a day after, also with no operational impact.

Taken together, the cases point to the same review areas: vendor access to data, the exposure of test and monitoring systems, and endpoint controls on shared or portable devices.

What to do now

1. Review which vendors hold copies of your data or configurations, and confirm contractual breach-notification duties and access removal after projects end.

2. Inventory public-facing status pages and dashboards, and check that they have no path into internal operations networks.
3. Apply production-grade access control and monitoring to test environments, and avoid keeping real customer data in them.
4. Treat device configuration snapshots shared with vendors as sensitive and confirm they are protected and retained only as needed.
5. For FastUnlock, restrict physical access to Windows 11 devices, track Microsoft guidance for a fix, and consider limiting Narrator use on high-risk shared devices.
6. Check incident response plans for third-party notification, including PDPL breach reporting where personal data is involved.