Hacking campaign targets FileZen file-sharing network appliances

therecord.media/hacking-campaign-targets-filezen-file-sharing-network-appliances/

April 25, 2021

Threat actors are using two vulnerabilities in a popular file-sharing server to breach corporate and government systems and steal sensitive data as part of a global hacking campaign that has already hit a major target in the Japanese Prime Minister's Cabinet Office.

The attacks target FileZen, a popular file-sharing network appliance from Japanese firm Soliton, and are eerily similar to the attacks that targeted Accellion's FTA file-sharing systems in late 2020, early 2021.

Both appliances work in the same manner. They are used to store large files that can't be sent via email. Users typically upload files on a FileZen server and then use a web-based panel to obtain links that they can share with fellow employees or persons outside of their organization.

Just like most of these vendors, Soliton provides a cloud-based version of FileZen, but also standalone servers that can be installed on-premises to meet certain data privacy requirements in highly secured environments.

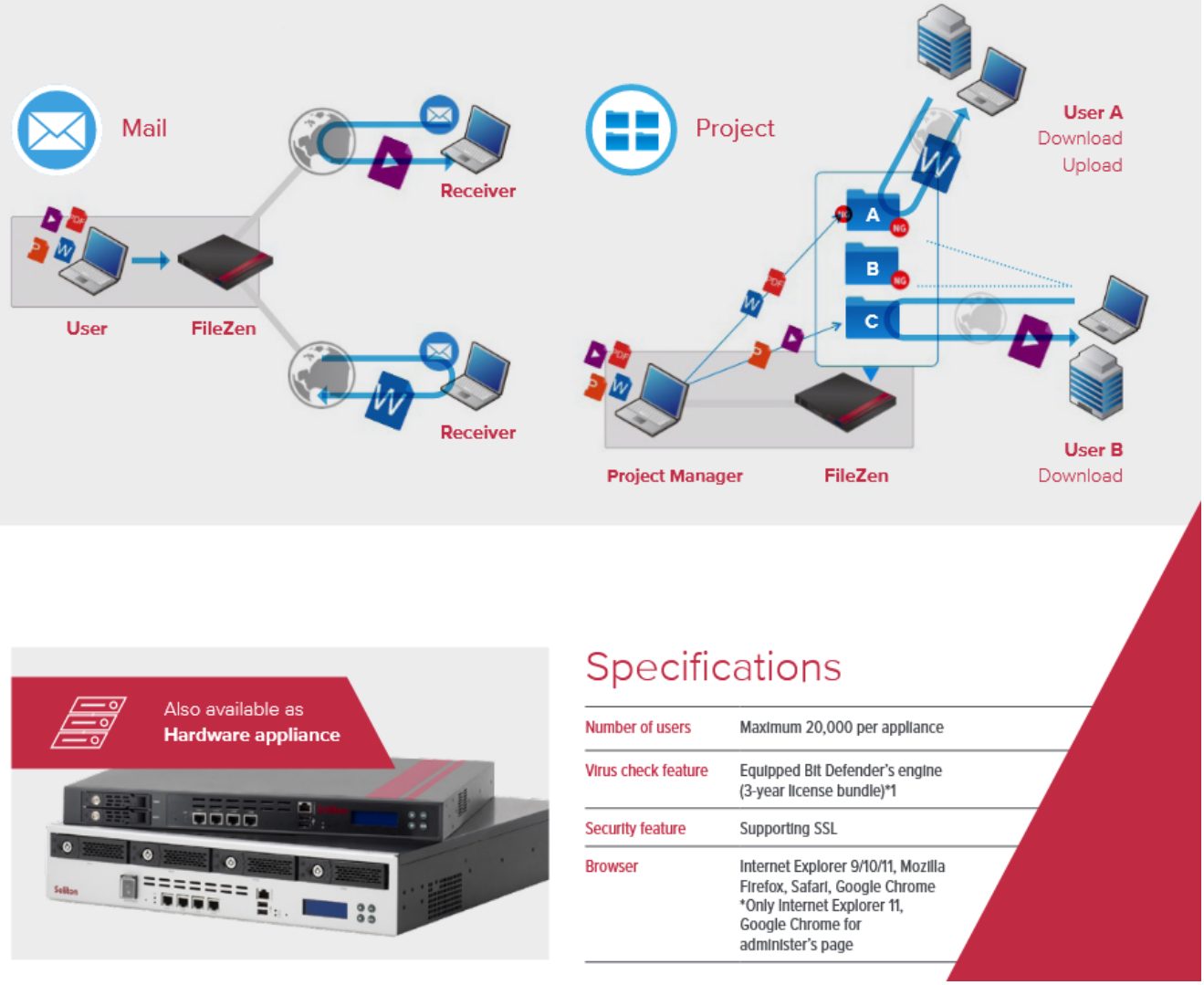

Image: Soliton

But while the FTA attacks came to light earlier this year, investigators are only now discovering the exploitation attempts that targeted FileZen, a solution that has a smaller install base, primarily located inside Japan.

Two vulnerabilities exploited in the wild

A source familiar with the investigation in Japan has told *The Record* that hackers appear to have found a combination of two FileZen security bugs, which they began exploiting earlier this year, in January.

Threat actors used CVE-2020-5639 and CVE-2021-20655—two vulnerabilities that have been patched in December 2020 and February 2021, respectively—to breach FileZen systems left connected online that have not been placed behind a firewall.

The first vulnerability allowed threat actors to upload malicious files on the device, while the second allowed them to run OS commands with elevated privileges.

In support documents published on its website, Soliton is telling customers to update to versions v4.2.8 or v5.0.3 or later to patch the attacker's point of entry and prevent future intrusions.

However, since the attacks started before a patch was ready, Soliton is also working on the presumption that customer systems have already been breached.

The company is now advising that customers reset all admin account passwords and reset access-control (internal firewall) lists.

The source told *The Record* that there was not enough evidence to link the attacks on FileZen devices to the earlier attacks that targeted FTA systems, but that this would not surprise investigators, as the FileZen attacks appear to have started just as the FTA attacks were publicly exposed and slowly died out.

Tags

- Accellion
- Asia
- Cabinet Office
- FileZen
- hacking campaign
- Japan
- Soliton
- vulnerability
- zero-day

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.