SSD Advisory – Horde Groupware Unauthorized File Download

blogs.securiteam.com/index.php/archives/3454

SSD / Maor Schwartz October 3, 2017

Vulnerability Summary

The following advisory describes an unauthorized file download vulnerability found in Horde Groupware version 5.2.21.

Horde Groupware Webmail Edition is “a free, enterprise ready, browser based communication suite. Users can read, send and organize email messages and manage and share calendars, contacts, tasks, notes, files, and bookmarks with the standards compliant components from the Horde Project. Horde Groupware Webmail Edition bundles the separately available applications IMP, Ingo, Kronolith, Turba, Nag, Mnemo, Gollem, and Trean.”

Credit

An independent security researcher, Juan Pablo Lopez Yacubian, has reported this vulnerability to Beyond Security’s SecuriTeam Secure Disclosure program.

Vendor response

Horde Groupware was informed of the vulnerability, to which they response with:
“this has already been reported earlier by someone else, and is already fixed in the latest Gollem and Horde Groupware releases.

Besides that, it’s not sufficient to have a list of the server’s users, you also need to exactly know the file name and path that you want to download. Finally, this only works on certain backends, where Horde alone is responsible for authentication, i.e. it won’t work with backends that require explicit authentication.”

Vulnerability details

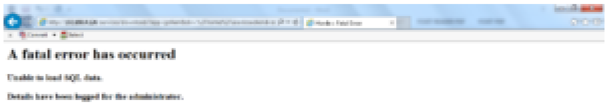
User controlled input is not sufficiently sanitized when passed to File Manager (gollem) module (version 3.0.11).

The “fn” parameter does not validate certain met characters by causing the requested file or filesystem to be downloaded without credentials.

It is only necessary to know the username and the file name.

Proof of Concept

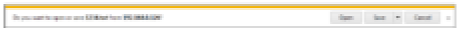
```
User = this is the username in horde
/ = the Meta character /
/services/download/?app=gollem&dir=%2Fhome%2Fuser&backend=sqlhome&fn=/test.php
```



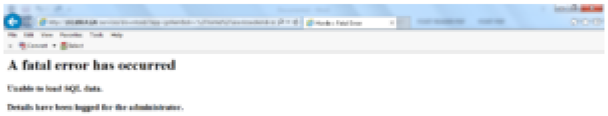
A fatal error has occurred

Unable to load SQL data.

Details have been logged for the administrator.



Do you want to open or save [illegible] from [illegible]?



A fatal error has occurred

Unable to load SQL data.

Details have been logged for the administrator.